VERINT

POWERING ACTIONABLE INTELLIGENCE®

SConfigurator

Version 6.0

User Guide

September 17, 2010

© 2010 Verint Systems Inc. All Rights Reserved Worldwide. www.verint.com/videosolutions

Revision Notice

This is the second release of this manual. This manual provides technical and editorial updates and replaces all previous editions. Please refer to the Summary of Changes for a complete revision history.

About This Document

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited. By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change.

Verint Systems Inc. does not warrant, guarantee or make any representation regarding the use or the results of the use of the information, links, tools, and materials in terms of the accuracy, reliability, quality, validity, stability, completeness, currentness, or otherwise of its content or products. The entire risk as to the use, results and performance of information, links, tools and materials provided or referenced herein is assumed by the user. Verint Systems Inc. shall not be liable for damages resulting from the use, misuse or unlawful use of the information, links, tools, and materials contained or referenced herein.

The Verint Systems Inc. products are protected by one or more of the following U.S., European or International Patents: USPN 5,659,768; USPN 5,689,442; USPN 5,790,798; USPN 6,278,978; USPN 6,370,574; USPN 6,404,857; USPN 6,510,220; USPN 6,724,887; USPN 6,751,297; USPN 6,757,361; USPN 6,782,093; USPN 6,839,667; USPN 6,952,732; USPN 6,959,078; USPN 6,959,405; USPN 7,047,296; USPN 7,149,788; USPN 7,155,399; USPN 7,203,285; USPN 7,216,162; USPN 7,219,138; USPN 7,254,546; USPN 7,281,173; USPN 7,284,049; USPN 7,325,190; USPN 7,466,816; USPN 7,478,051; USPN RE40,634; and other provisional rights from one or more of the following Published US Patent Applications: US 11/394,408; US 11/771,499; US 11/396,514; US 11/772,440; US 11/565,943; US 11/565,946; US 11/565,948; US 11/540,739; US 11/540,086; US 11/541,313; US 11/541,252; US 11/540,282; US 11/529,947; US 11/540,785; US 11/540,736; US 11/540,904; US 11/540,353; US 11/608,340; US 11/608,350; US 11/608,358; US 11/567,808; US 11/692,983; US 11/693,933; US 11/693,923; US 11/693,828; US 11/567,852; US 11/608,440; US 12/015,621; US 11/540,322; US 11/924,201; US 11/616,490; US 11/621,134; US 11/752,458; US 11/712,933; US 11/824,980; US 11/729,185; US 11/804,748; US 11/831,260; US 11/395,992; US 11/359,319; US 11/359,195; US 11/359,357; US 10/832,509; US 11/742,733; US 11/831,257; US 11/831,250; US 11/691,530; US 11/479,267; US 11/529,942; US 11/768,349; US 11/540,281; US 10/633,357; US 11/693,899; US 11/479,056; US 11/529,132; US 11/540,320; US 11/037,604; US 11/529,842; US 11/540,171; US 11/478,714; US 11/529,946; US 11/868,656; US 11/776,659; US 11/090,638; US 11/410,004; US 10/771,315; US 10/771,409; US 11/540,900; US 11/528,267; US 12/118,781; and other U.S. and International Patents and Patents Pending.

VERINT, the VERINT logo, ACTIONABLE INTELLIGENCE, POWERING ACTIONABLE INTELLIGENCE, WITNESS ACTIONABLE SOLUTIONS, STAR-GATE, RELIANT, VANTAGE, X-TRACT, NEXTIVA, ULTRA, AUDIOLOG, WITNESS, the WITNESS logo, IMPACT 360, the IMPACT 360 logo, IMPROVE EVERYTHING, EQUALITY, CONTACTSTORE, and CLICK2STAFF are trademarks or registered trademarks of Verint Systems Inc. or its subsidiaries. Other trademarks mentioned are the property of their respective owners.

Contents

Preface iii
Chapter 1: Getting Started 1
Starting SConfigurator 2
Changing SConfigurator Parameters 4
Configuring the IP Network for SConfigurator 4
Configuring SSL for SConfigurator 6
Discovering Edge Devices 7
Choosing Information to Display 11
Chapter 2: Configuring the Edge Devices 13
Presenting the Configuration Parameters 14
Accessing the General Parameters 15
Configuring IP 17
Configuring VSIP 19
Configuring SSL 21
Setting the SNMP Properties 22
Configuring NTP 24
Configuring Wireless 25
Configuring Wireless Communication 25
Configuring Wireless Security 29
SPCF and SDCF 29
802.11 30
Accessing the Link Status 33
Selecting Multicast Filters 34
Configuring Video 35
Configuring the Video Standard 35
Configuring the Treatment of Color on an Input 36
Configuring an Encoder 37
Configuring the Brightness of a Receiver 41
Configuring the Serial Port 42
Configuring Audio 44
Configuring the Sampling Rate 44
Configuring an Audio Encoder 45
Configuring an Audio Decoder 46
Configuring the S4100 Series 47
Preparing the Configuration 47
Assigning Initial Parameters 49
Performing an Advanced Configuration 51
Resetting the Configuration 56
Configuring the S1816e-SP Encoder 57

Performing a Batch Network Configuration 59

Chapter 3: Managing Connections 62
Adding a Connection 63
Removing a Connection 65

Chapter 4: Enabling Security 66
Building a Secure System 67
Adding a Device to the Trusted List 68

Chapter 5: Updating Firmware 69
Performing the Update 70
Firmware Update Messages 71

Chapter 6: Aligning the Antenna 73
Aligning the External Antenna 74

Chapter 7: Managing the Licenses 75
Creating a License Request File 76
Installing Licenses 77
Assigning a Package 79
Removing a License 81

Chapter 8: Troubleshooting an Edge Device 82
Troubleshooting 83

Appendix A: DHCP Support and APIPA 85
Appendix B: Accessing the CLI 87
Glossary 90

Preface

The *Verint SConfigurator User Guide* presents the information and procedures for configuring the Nextiva® edge devices using SConfigurator:

- Wired video receivers and transmitters:
  - S1504e-R receiver
  - Multiport S1700e series transmitters covering the S1704e, S1704e-AS, S1708e, S1708e-AS, S1712e, and S1724e
  - Multiport S1800e series transmitters covering the S1808e, S1816e and S1816e-SP
  - Single/Dual port S1800e series transmitters and receivers covering the S1801e, S1801e-POE, S1801e-R, S1801e-R-HD, S1802e.
  - S1900e series covering the S1900e-AS, S1950e, and S1970e transmitters and the S1970e-R receiver
- IP cameras:
  - S1900e-Vicon (to create the Nextiva-Vicon camera)
  - S2500e
  - S2600e series covering the S2600e, S2600e-AS, S2610e, and S2610e-AS
  - S2700e series covering the S2700e and S2700e-VR
  - S2750e series covering the S2750eN and S2750eP
  - S5000 series covering the S5003BX, S5003FD, S5003FDW, S5020BX, S5020FD and S5020FDW.
- Wireless video transmitters:
  - S1100w
  - S4200 series covering the S4200, S4200-AS, S4200-2V, and S4200-AS-2V
- Wireless transmitter/receiver system—S4100 series covering the S4100 and S4100-2V
- Multipurpose outdoor wireless devices:
  - S3100 series covering the S3100, S3100-BR, and S3100-RP
  - S4300 series covering the S4300, S4300-BR, and S4300-RP

Audience

This guide has been prepared for the following audience:

- Managers
- IT system administrators
- Engineers
- Technicians

Contacting Verint

Verint® Systems is a leading provider of Actionable Intelligence® solutions for enterprise workforce optimization and security intelligence. Our solutions help government and enterprises make sense of the vast information they collect in order to achieve their performance and security goals. Today our solutions are used by more than 10,000 organizations in 150 countries. Verint is headquartered in Melville, New York, with offices worldwide and 2500 dedicated professionals around the globe. You can read about Verint Video Solutions and get marketing material and product information at www.verint.com/videosolutions.

▶ To contact us for sales, pricing and general inquiries:

- The Americas:
  - **EMAIL**: videoinfo@verint.com
  - **TELEPHONE**: +1 866-639-8482 for Nextiva Enterprise and Nextiva Intelligent Edge Devices
  - **TELEPHONE**: +1-800-638-5969 for Nextiva embedded DVRs
- Europe, the Middle East, or Africa:
  - **EMAIL**: marketing.emea@verint.com
  - **TELEPHONE**: +44 (0) 1932 839500
- Asia Pacific:
  - **EMAIL**: marketing.apac@verint.com
  - **TELEPHONE**: + 852 2797 5678

Contacting Service and Support

To request the latest versions of firmware and software or to download other product-related documents, you need access to the Verint Video Intelligence Solutions partner extranet. To register, go to https://ve5.verint.com.

If you encounter any type of problem after reading this guide, contact your local distributor or Verint representative. For the main service and support page on the Verint web page, visit www.verint.com/videoservice. For assistance, use our online web form at http://verint.com/video_solutions/info/57008 or contact the customer service team:

Location	Telephone	E-mail	Opening hours
USA and Canada	+1-888-747-6246 +1-888-585-7059	vissupport@verint.com CLM_Customersupport@verint.com	8:00 am to 8:00 pm (EST) Monday to Friday
Central and Latin America	+1-303-254-7005	vissupport@verint.com	
Europe, Middle East, and Africa	+44 (0) 845-843-7333	customersupport.emea@verint.com	8:30 am to 5:30 pm (GMT) Monday to Friday

Location	Telephone	E-mail	Opening hours
	+49 (0) 4321-269 81 36	mobilesupport@verint.com (Transit applications only)	
Asia/Pacific	Hong Kong: +852 2797 5678 Singapore: +65-68266099	APAC_VIS_Services@verint.com	9:00 am to 6:30 pm (Monday to Thursday); 9:00 am to 5:30 pm (Friday)

Related Documentation

Download the documentation and SConfigurator Utility: www.verint.com/manuals.

Download the latest firmware from the extranet: http://vvs.verint.com.

Send your questions or comments on the current document, or any other Nextiva user documentation, to our documentation feedback team at documentationfeedback@verint.com.

Chapter 1

Getting Started

Starting SConfigurator 2
Changing SConfigurator Parameters 4
Discovering Edge Devices 7
Choosing Information to Display 11

SConfigurator is a PC-based administration tool for use over any TCP/IP network. It is built on open standards to provide long-term investment protection. You use SConfigurator to:

- Configure Nextiva edge devices
- Add security in your system
- Get information on the devices connected on the network
- Connect edge devices together
- Access the command line interface of the devices
- Update the firmware of the devices
- Align the antennas of wireless devices
- Manage licenses

Before starting to configure Nextiva edge devices, you need to:

- Configure the parameters for the IP network and SSL (Secure Sockets Layer) security
- Discover edge devices on the network
- Choose information to display

Starting SConfigurator

The latest version of the SConfigurator tool is available on the Verint web site: www.verint.com/manuals.

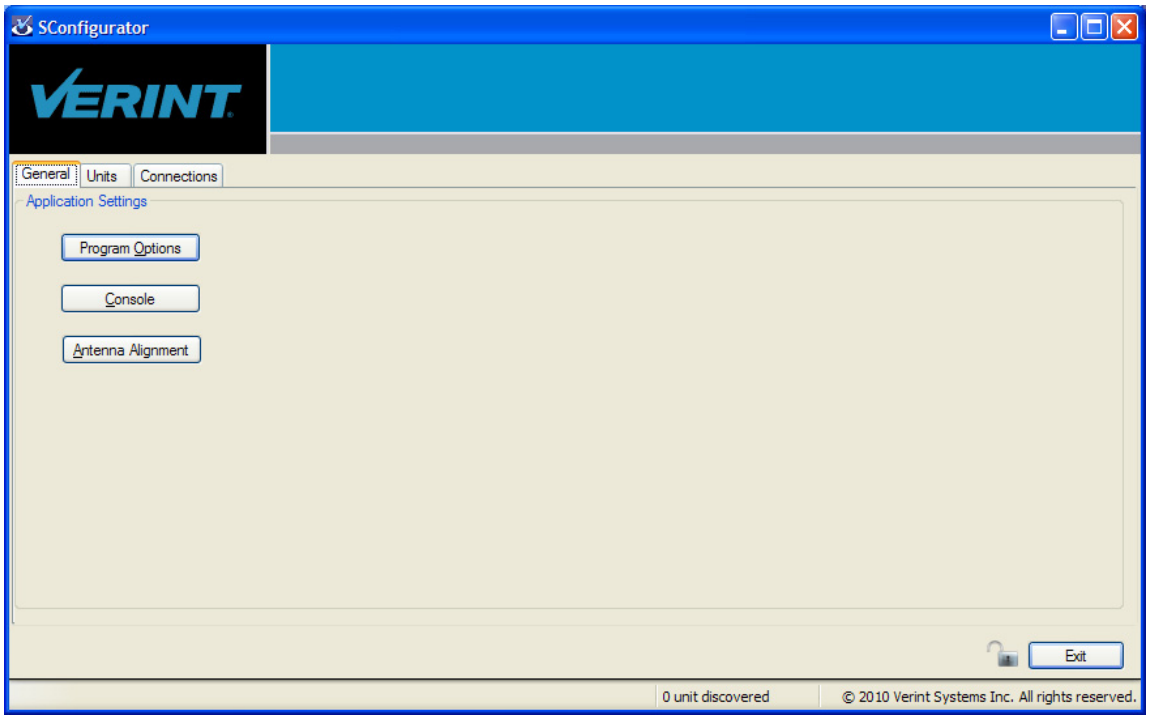
The minimum software and hardware requirements for the computer needed to use SConfigurator are:

- Windows 2000 Service Pack 2 or higher, or Windows XP
- An Ethernet network card
- A serial port (not through a USB converter)

▶ To start SConfigurator:

1. Each time you have a new software version, copy the `SConfigurator.exe` file to the hard disk of your computer.
2. In the Windows file manager, start the `SConfigurator.exe` program.

The SConfigurator window appears.



3. To change SConfigurator options, access the command line interface (CLI), and align the antennas of wireless devices, click the **General** tab.
4. To get an inventory of the Nextiva edge devices on the IP network, configure them, and perform firmware updates, click the **Units** tab.
5. To manage point-to-point connections between a transmitter and a receiver, click the **Connections** tab.

Changing SConfigurator Parameters

You can change the SConfigurator parameters relative to the IP network and to SSL.

Configuring the IP Network for SConfigurator

The following SConfigurator parameters are mainly used to discover Nextiva devices on the IP network; for more information about the discovery process, see *page 7*. The parameters are:

- IP Address of the PC—The unique IP address of the computer where SConfigurator runs. You do not normally have to change this value, since SConfigurator automatically detects it. However, you can change the displayed value if:
  - You are using two Ethernet cards on your PC.
  - You are using a virtual private network (VPN).
  - The IP address of the computer has changed.
- Detect All Units on LAN—The indication of whether all devices connected to the same LAN as the PC and having the same VSIP port as SConfigurator will be discovered, even those whose IP addresses are not part of the same subnet as the computer.

NOTE: This parameter works only with the broadcast detection method. If you select it, SConfigurator automatically switches to broadcast, even if the Discovery IP Address box displays the multicast address.

  You typically activate this parameter to discover the new devices on the network and those in APIPA mode (for more information, see *Appendix A: DHCP Support and APIPA*). When this parameter is activated, device discovery takes more time.
- VSIP Port—The communication port used for VSIP (Video Services over IP) command-and-control messaging between SConfigurator and Nextiva devices. This port number must be the same in SConfigurator and in the devices to be configured. The default VSIP port is 5510.

NOTE: VSIP ports 9541, 65500, and those under 1024 are reserved and should never be used, not even for serial port, video, or audio communication. The maximum value is 65535.

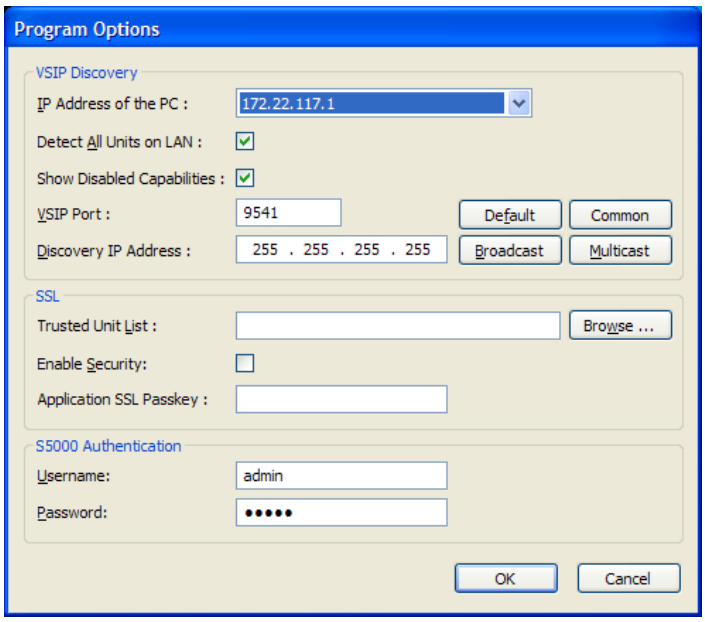
  All devices and SConfigurator also have the ability to receive messages on a hard-coded VSIP port, 9541, called the *common* port. The common port is typically used for troubleshooting, when you lost the VSIP port of devices.

  Unless otherwise specified, the phrase *VSIP port* refers to the configurable port and not to the common port.
- Discovery IP Address—The communication method and associated IP address SConfigurator will use to detect Nextiva devices on the network. Contact your system administrator to know which method your network supports. Possible methods are:

- Broadcast—Sending a message to all devices physically connected to the same network as SConfigurator; it may not reach devices on other LANs. The broadcast IP address is 255.255.255.255. (Default)
- Multicast—Sending a message to a selected group of devices. With the multicast method, SConfigurator can discover devices located across multiple networks, but not through the Internet. The current multicast IP address is 224.16.32.1 and should not be changed.

▶ To change the SConfigurator IP network parameters:

1. In the General tab, click **Program Options.** The Program Options window appears.



2. Select the IP address of the correct LAN interface from the **IP Address of the PC** list.
3. To change the configurable VSIP port, do one of the following steps:
   - In the **VSIP Port** box, type its new value.
   - To reset it to its default value (5510), click **Default**.
   - To set it to the common value (9541) for troubleshooting, click **Common**.
4. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast** or click **Multicast** to set it to 224.16.32.1.
5. In the S5000 Authentication section, type the username and password for the Nextiva S5000.

NOTE: The default username and password for the Nextiva S5000 is admin.

6. Click **OK**.

Configuring SSL for SConfigurator

You can enable the SSL protocol between SConfigurator and Nextiva devices. This way, VSIP communication occurring on the IP network will be secure. For more information about SSL, see *Enabling Security* on *page 66*.

By default, SConfigurator can communicate with devices holding an SSL certificate (*SSL-enabled* devices) as well as non-SSL devices. However, you can increase security by forcing SConfigurator to communicate only with SSL-enabled devices that it trusts and that share the same SSL passkey.

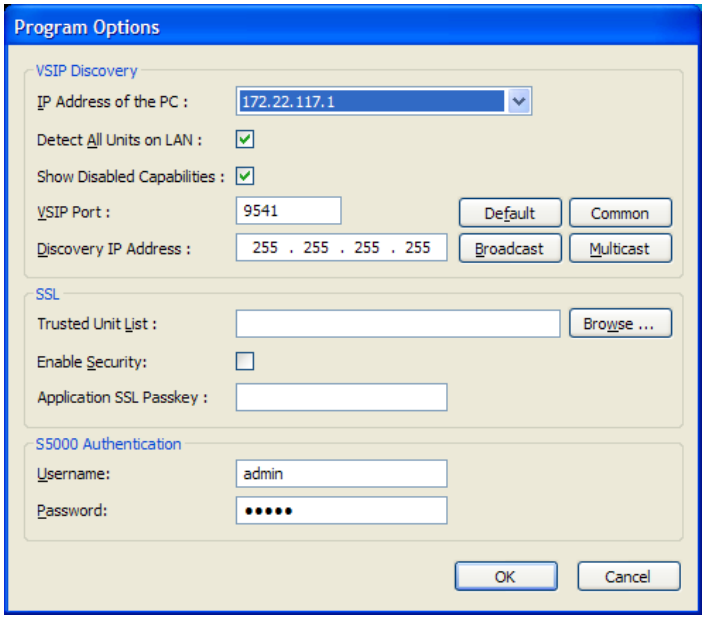
The SConfigurator SSL parameters are:

- Trusted Unit List—The list of trusted Nextiva devices that SConfigurator will manage in a secure system.
- Enable Security—The indication of whether SConfigurator communicate only with SSL-enabled devices that are included in the trusted list and share the same SSL passkey.
- Enter SSL Passkey—To change the password shared by SConfigurator and SSL-enabled devices to establish a secure VSIP connection.

▶ To change the SConfigurator SSL parameters:

1. In the General tab, click **Program Options.**

   The Program Options window appears.



2. To create an empty trusted unit list:
   a. In the SSL box, click **Browse**.
   b. Select the directory that will hold the list.
   c. In the **File name** box, enter a meaningful name, then click **Open**.

   The path and name of the list appear in the Trusted Unit List box.
3. To change the trusted unit list, click **Browse**, then select the desired file.
4. To force SConfigurator to communicate only with SSL-enabled devices that are part of the trusted list, check **Enable Security**.

5. To change the SSL passkey:
   a. Click **Enter SSL Passkey**.
      The SSL Passkey window appears.
   b. Type the passkey, then click **OK**.
   You will need to enter this passkey each time you start SConfigurator in secure mode.
6. Click **OK**.

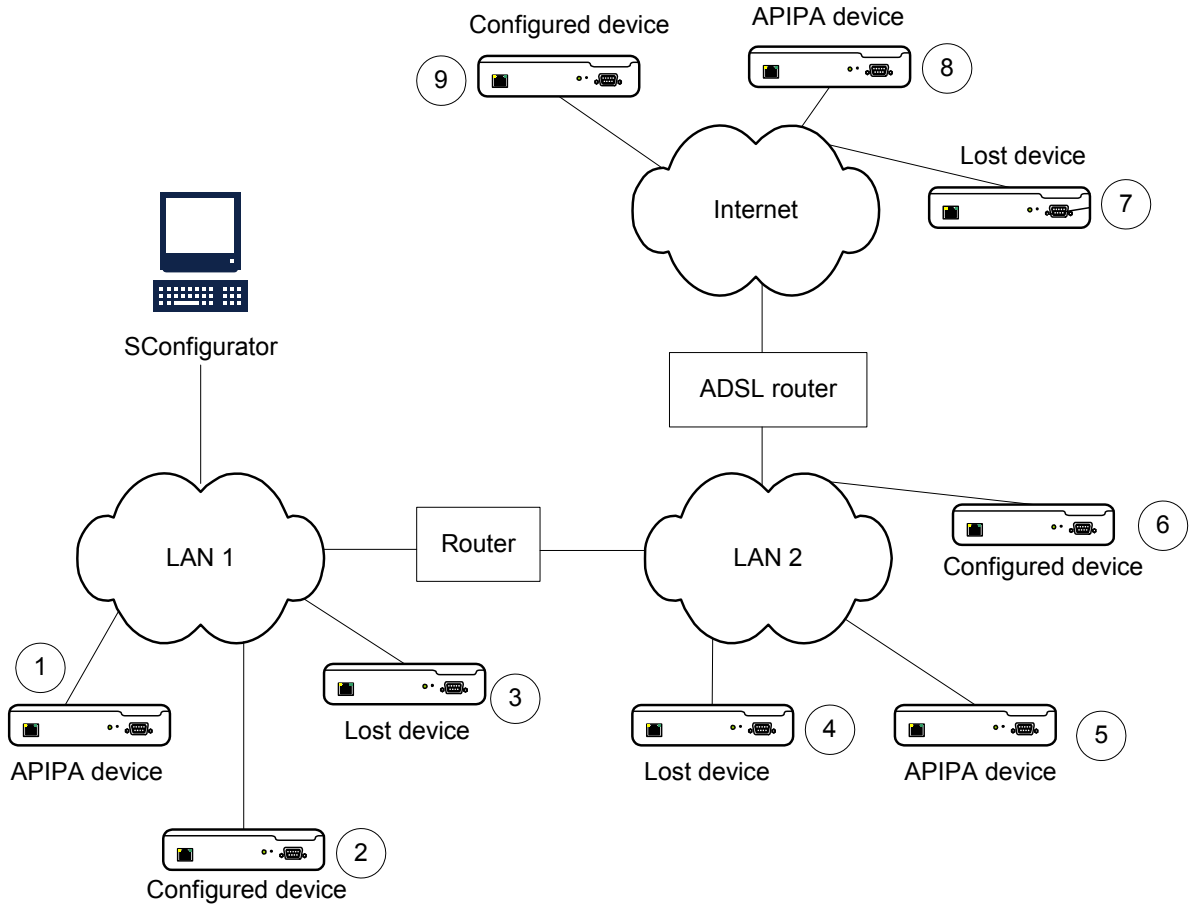
Discovering Edge Devices

The Units tab displays the devices that have been discovered by SConfigurator on the IP network. The number of devices found varies depending on the following parameters (for their description, see *page 4*):

- The communication method used to detect devices on the network:
  - Broadcast—A message is sent to all devices physically connected to the same network.
  - Multicast—A message is sent by a single sender to multiple receivers.
  - Unicast—A message is sent by a single sender to a single receiver.
- The VSIP port
- The Detect All Units on LAN parameter

Regardless of the number of devices to discover, you should take into account the SSL security status in SConfigurator (described in *Configuring SSL for SConfigurator* on *page 6*).

To present the discovery scenarios, consider the following network configuration:



Three types of Nextiva devices are presented:

- A properly configured device having the same VSIP port as SConfigurator (*Configured device*)
- A device in APIPA mode: A brand new device, a device having been through a factory reset, a device with a duplicate IP address, or a device unable to receive an address from a DHCP server (*APIPA device*)

  For more information about APIPA, see *Appendix A: DHCP Support and APIPA*.
- A device whose VSIP port and IP address are unknown (*Lost device*)

The following discovery scenarios are available:

Broadcast	Multicast	Unicast	Common VSIP Port	Detect All Units on LAN	Discovered Devices
P					2
P				P	1, 2

Broadcast	Multicast	Unicast	Common VSIP Port	Detect All Units on LAN	Discovered Devices
P			P		2, 3
P			P	P	1, 2, 3
	P			n/a	2, 6
	P		P	n/a	2, 3, 4, 6
		P		n/a	2, 6, 9
		P	P	n/a	2, 3, 4, 6, 7, 9

With the broadcast method:

- SConfigurator can find devices only on the local network, provided they share the same VSIP port (device 2).
- The Detect All Units on LAN parameter works only in broadcast mode. This parameter helps detect the APIPA device (device 1), which resides on a subnet different from that of the computer. Their VSIP ports need to be the same.
- The common port is required to find the lost device (device 3), since its configured VSIP port is different from SConfigurator's.

With the multicast method:

- SConfigurator can locate configured devices attached to remote networks (device 6, provided they share the same VSIP port), but not through the Internet.
- SConfigurator cannot find the APIPA devices (devices 1 and 5), since they require the Detect All Units on LAN parameter available only with the broadcast method.
- The common port helps locate the lost devices (devices 3 and 4).

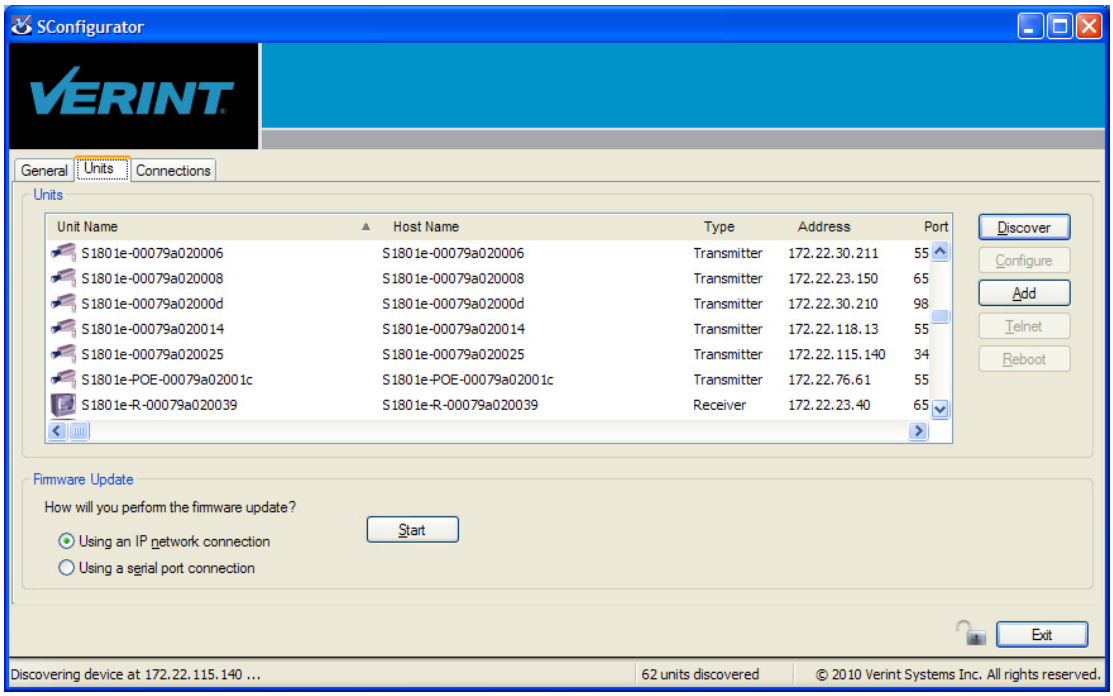
With the unicast method:

- Each configured device is discovered individually. Typically, you use unicast when the device cannot be located with the broadcast or multicast methods.
- SConfigurator can detect all devices sharing the same VSIP port, even those accessible only through Internet (device 9), provided you know their individual IP addresses.
- SConfigurator cannot locate the APIPA devices (devices 1, 5, and 8) since they require the Detect All Units on LAN parameter available only with the broadcast method.
- The common port helps locate the lost devices (devices 3, 4, and 7).

In the Units tab, you use the Discover button to find many devices with the broadcast or multicast method (depending on the Discovery IP Address parameter in the program options). To discover a single device with the unicast method, you use the Add function. Be aware however that most unicast-discovered devices will disappear from the Units box the next time you click Discover, since the list is emptied before the broadcast or multicast command is launched.

To discover devices with the broadcast or multicast method:

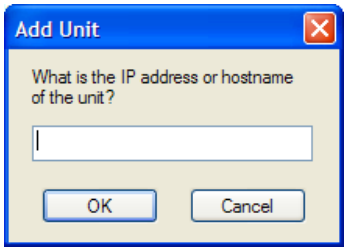
- In the Units tab, click **Discover**. The discovered devices appear in the Units box.



If devices of type Unknown appear, see *Chapter 8: Troubleshooting an Edge Device* for the probable causes.

To find a specific device with the unicast method:

1. In the Units tab, click **Add**. The Add Unit window appears.



2. Enter the IP address or host name of the device you want to find, then click **OK**.

The device is added to the Units box.

Choosing Information to Display

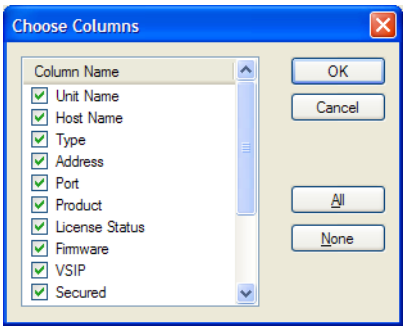
You can select the columns that will appear in the Units box. The available columns are:

- Unit Name—A meaningful name given to the device (see *page 15*).
- Host Name—An alias for the IP address of the device, as provided in the Network>IP tab (see *page 17*).
- Type—The function of the device. The available values are: Receiver, Transmitter, and Access Point.
- Address—The IP address of the device.
- Port—The configurable VSIP port of the device.
- Product—The type of the Nextiva device (for example, S1100w, S3100, and so on).
- License Status—The status of the license that can be installed in the device. For more information, see *Chapter 7: Managing the Licenses*. The available values are:
  - Not Installed: The device supports licensing but either the license is not yet installed or the device underwent an upgrade with a new firmware that supports licensing (default).
  - Not Supported: The device does not support licensing.
  - Valid: The license is installed properly.
- Firmware—The version of the firmware in the device.
- VSIP—The type of VSIP connection between the device and SConfigurator. The available values are:
  - UDP—A connection type used for point-to-multipoint messaging. It is not used anymore and remains for backward compatibility only.
  - TCP—An error-free connection (default).
  - SSL—A TCP connection secured with SSL.
- Secured—The indication of whether the Enable Security option is enabled in the device (see *page 21*).
- Trusted—The indication of whether the device is part of the trusted list (for more information, see *page 6*).
- Temp (°C)—The internal board temperature.
- Uptime—The time the device has been running since it was booted.
- MAC Address—The hardware address of the device on the network.

▶ To choose the information to display:

1. Click the **Units** tab.
2. In the Units box, right-click any device.

3. From the contextual menu, choose **Choose Columns**. The Choose Columns window appears.



4. Select the desired columns, then click **OK**.

Chapter 2

Configuring the Edge Devices

Presenting the Configuration Parameters 14
Accessing the General Parameters 15
Configuring IP 17
Configuring VSIP 19
Configuring SSL 21
Configuring NTP 24
Configuring Wireless 25
Selecting Multicast Filters 34
Configuring Video 35
Configuring the Serial Port 42
Configuring Audio 44
Configuring the S4100 Series 47
Configuring the S1816e-SP Encoder 57
Performing a Batch Network Configuration 59

You can perform the following tasks in the Units tab of the SConfigurator window:

- Configuring edge devices
- Performing a batch network configuration

Presenting the Configuration Parameters

SConfigurator allows you to change or display several parameters in the devices:

Parameters	Multiport S1800e Series	S1504e-R, Multiport S1700e Series	S1900e Series	S1100w, S4200 Series	S1900e-Vicon, S2500e, S2600e Series, S2700e Series,	S3100 Series, S4300 Series
General	P	P	P	P	P	P
Network						
• IP, VSIP, SSL, NTP	P	P	P	P	P	P
• Wireless				P		P
• Filters						P
• Link status						P
Video	P	✓	P	P	P	
Serial port	P	P	P	P		
Audio		Optional	P	P		

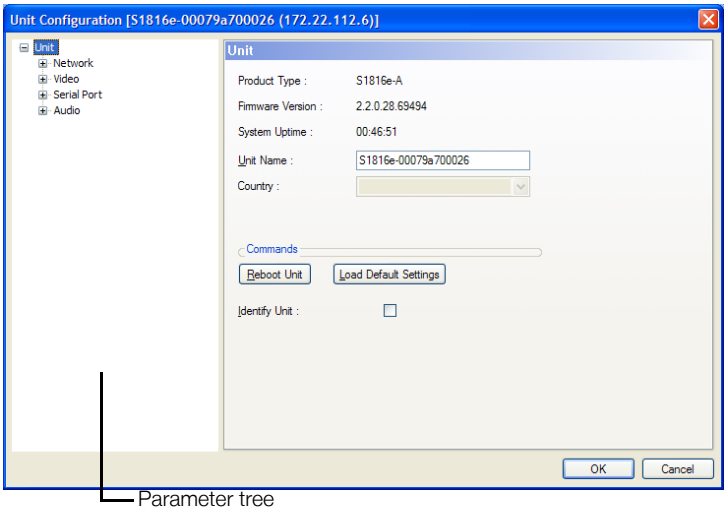
Typically you will use the edge devices with a video management software. In that context, you need S1900e-Vicon for the initial configuration only; other categories of parameters may be overwritten by the software. The only exceptions are:

- The S4100 series uses a different set of pages for configuration. For more information, see *page 47*.
- The S1100 devices use the Verint Configuration Assistant tool for configuration. However, you may have to use SConfigurator to change their wireless parameters when the devices are part of a repeater setup. For more information, refer to the Verint *S1100 User Guide*.
- The S1800e Series devices use the new Web Interface for configuration. SConfigurator should only be used to obtain the IP address of the devices.

▶ To access the configuration parameters:

1. In the Units box, double-click the desired device.

   A Unit Configuration window appears.



2. In the parameter tree, click the desired node, then make the necessary changes. You may have to expand a node by clicking the plus (+) sign to its left.
3. Click **OK**.

Each time you change one or more parameters then click **OK**, a confirmation window appears. After you confirm the changes, the device may reboot.

Accessing the General Parameters

At the root of the parameter tree, in the Unit node, system status information on the device is available: product type, firmware version, and uptime.

You can also change the following parameters:

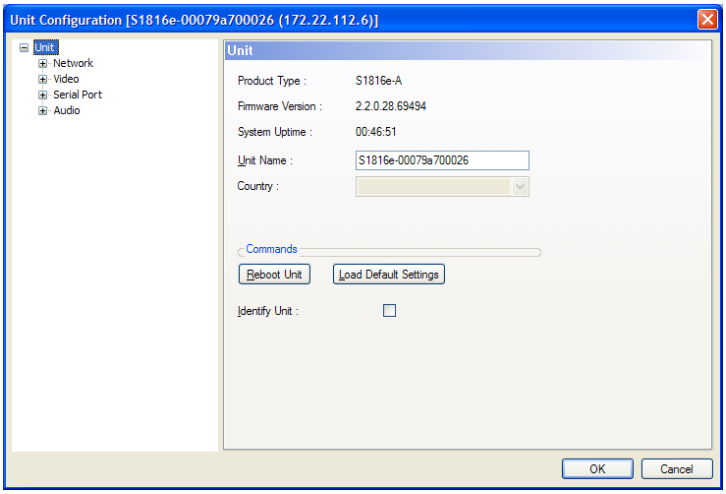
- For the S1100, S1100w, S3100 series, S4200 series, and S4300 series, you may have to set the country of operation. Depending on the country, the available frequency bands may differ, and the DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) regulations may apply. For more information about these regulations, refer to the user guide of the device.
- You should assign a meaningful name to every device. This name will be displayed in the Units box, under the Unit Name column.

Finally, the Unit node allows you to execute the following operations:

- Identify the device—Makes the status LED of the device flash red rapidly to recognize it among a large set of devices.
- Reboot the device—Performs a warm boot of the device. This operation will keep the current device configuration.
- Load default settings—Resets all configuration parameters to their factory settings. For a list of these values, refer to the “Factory Default Configuration” appendix in the user guide of the device.

▶ To access the general parameters:

1. In the parameter tree, click **Unit**.



2. To change the name of the device, enter a meaningful name in the **Unit Name** box.
3. To select the country of operation of a wireless device:
   a. In the **Country** list, select the country of operation of the device.
   b. In the confirmation window, click **Yes**.
4. To reboot the device or load its default parameters:
   a. Click **Reboot Unit** or **Load Default Settings** respectively. A confirmation message appears.
   b. Click **Yes**.
5. To identify the device:
   a. Check **Identify Unit**. The status LED flashes red.
   b. To reset the LED to its previous state, clear **Identify Unit**.
6. Click **OK**.

Configuring IP

The Network>IP node allows you to set a series of IP network parameters:

- Use DHCP—The indication of whether a DHCP (Dynamic Host Configuration Protocol) server will be used to provide a valid network configuration for your device. For more details, see *Appendix A: DHCP Support and APIPA*.

  DHCP provides the IP address, subnet mask, and gateway information.
- Use APIPA— The APIPA (Automatic Private IP Addressing) scheme, available on the Windows operating systems, allows a device to assign itself a temporary IP address until it receives a complete network configuration, either manually or from a DHCP server.
- IP Address—The unique 32-bit IP address of the device.
- Subnet Mask—The binary configuration that specifies the subnet in which the IP address of the device belongs. A subnet is a portion of a network that shares a common address component. Unless otherwise specified by your network administrator, it is recommended that you use a subnet mask of 255.255.0.0.
- Gateway—The IP address of your gateway. A gateway represents a network point that acts as an entrance to another network. Contact your network administrator for the correct gateway information.
- Host Name—An alias for the IP address of the device, to be used by the DNS server in a DHCP context. It is made up of 2 to 24 alphanumerical characters; the first one must be a character. This parameter is optional.

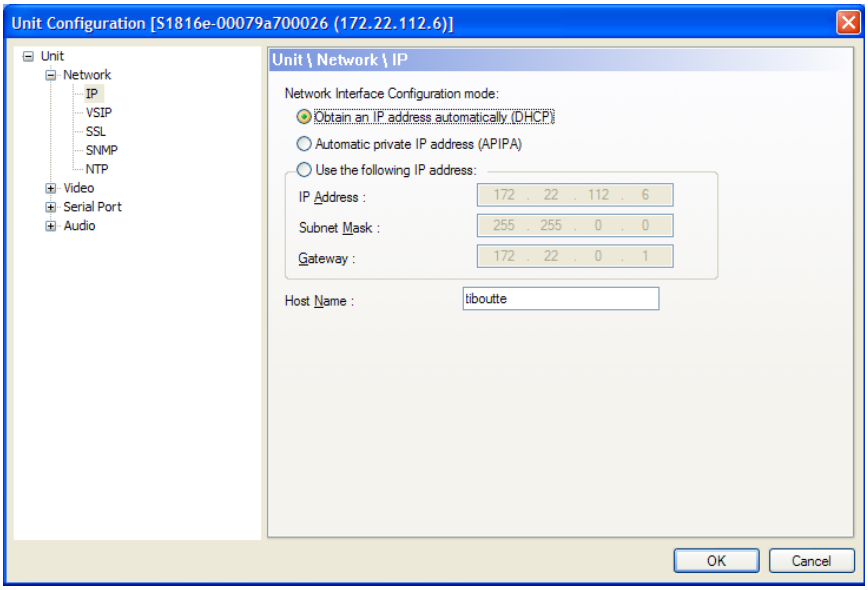
NOTE: It is up to the DHCP server to register the host name in the DNS server.

You can perform a batch network configuration if you have many devices to configure. For the procedure, see *page 59*.

▶ To use DHCP to change the IP network parameters:

1. In the parameter tree, expand the **Unit > Network** node, then click **IP**.

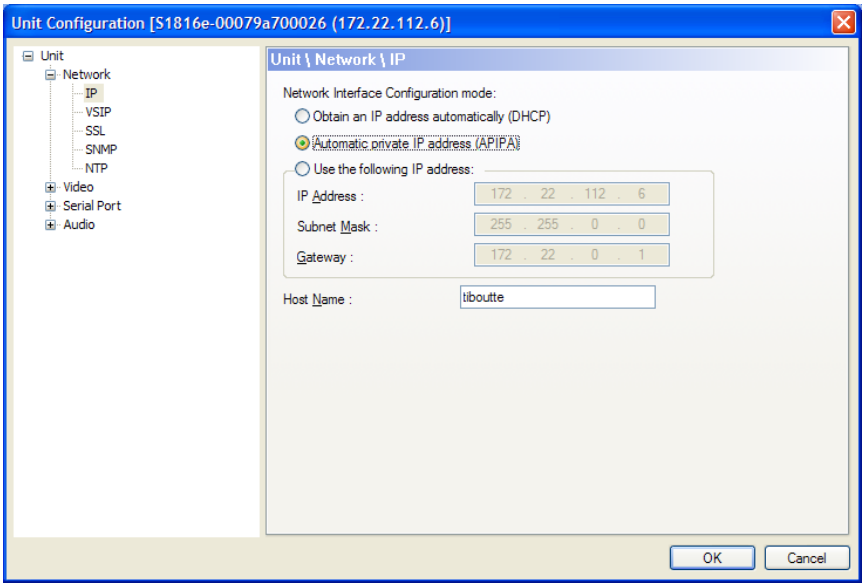
2. Check **Obtain an IP address automatically (DHCP)**. The IP Address, Subnet Mask, and Gateway boxes become unavailable.



3. If required, enter an alias in the **Host Name** box.
4. Click **OK**.

▶ To use APIPA:

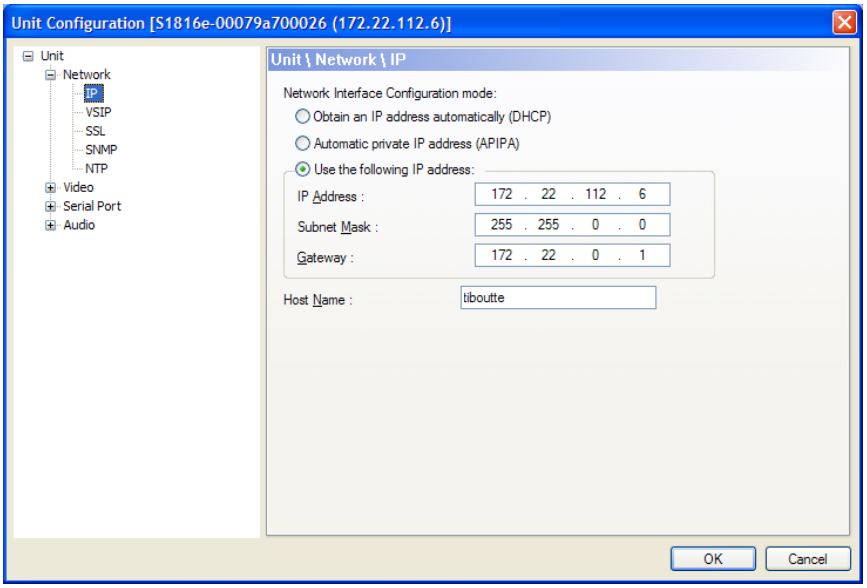
1. In the parameter tree, expand the **Unit > Network** node, then click **IP**.
2. Check **Automatic private IP address (APIPA)**. The IP Address, Subnet Mask, and Gateway boxes become unavailable.



3. If required, enter an alias in the **Host Name** box.
4. Click **OK**.

▶ To change the IP network parameters without DHCP:

1. In the parameter tree, expand the **Unit > Network** node, then click **IP**.
2. Select **Use the following IP address**.



3. In the **IP Address** box, enter the IP address of the device.
4. In the **Subnet Mask** box, enter the binary configuration specifying in which subnet the IP address of the device belongs.
5. If required, enter the IP address of the gateway in the **Gateway** box.
6. Click **OK**.

Configuring VSIP

The Network>VSIP node contains the parameters related to the proprietary VSIP (Video Services over IP) communication protocol. The values of these parameters must be the same in the device and in SConfigurator.

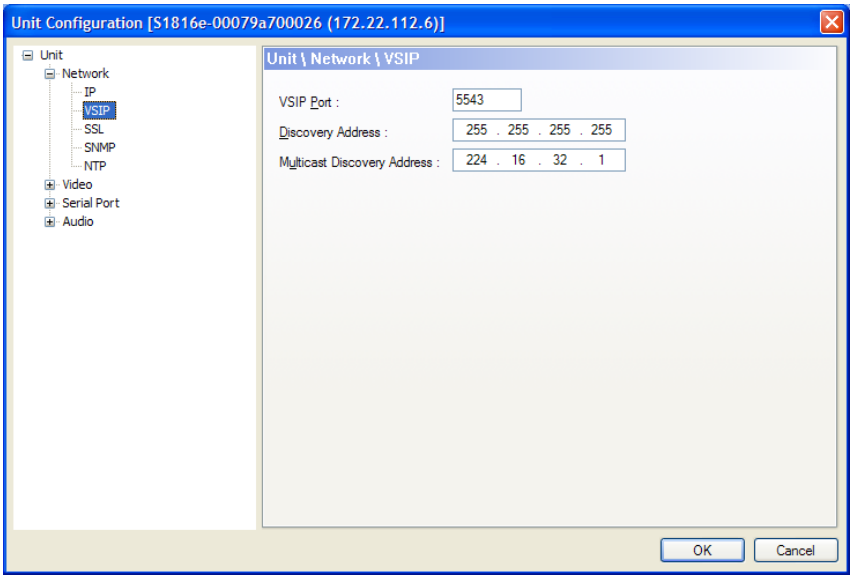
- VSIP Port—The VSIP port used by the device to communicate with SConfigurator. The default value of all Verint devices is 5510.

NOTE: VSIP ports 9541, 65500, and those under 1024 are reserved and should not be used, not even for serial port, video, or audio communication. The maximum value is 65535.

- Discovery Address—The IP address used by the device to make its presence known to SConfigurator with the broadcast method. With this method, S1900e-Vicon sends messages to all devices physically connected to its network. The broadcast address is 255.255.255.255.
- Multicast Discovery Address—The IP address used by the device to make its presence known to SConfigurator with the multicast method. With multicast, only a selected group of devices receives S1900e-Vicon messages. The current multicast address is 224.16.32.1 and should not be changed.

To change the VSIP parameters:

1. In the parameter tree, expand the **Unit > Network** node, then click **VSIP**.



2. Change the desired parameters.
3. Click **OK**.

Configuring SSL

Devices with an SSL digital certificate have the option of accepting only secure VSIP connections. Once a device is in secure mode, you cannot access it anymore with Telnet, you cannot perform firmware updates through the IP network on it, and you access its web interface (if applicable) in secure mode only.

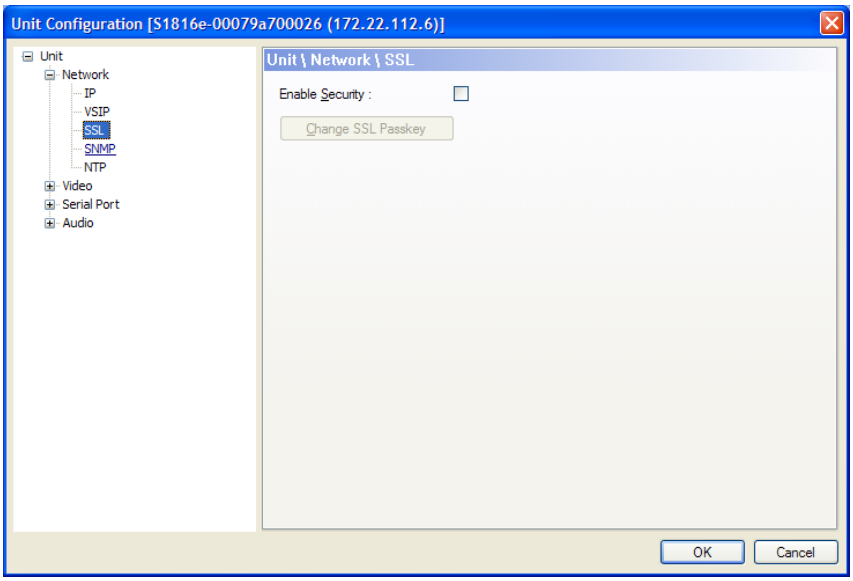
To enable SSL security on the device, the parameters are:

- Enable Security—The indication of whether the device only accepts SSL VSIP connections.
- Change SSL Passkey—To change the password shared by SConfigurator and all SSL-enabled devices to establish a secure system. You can change it only if the connection between the device and SConfigurator is secure.

For more information about SSL, see *Chapter 4: Enabling Security*.

▶ To change the SSL parameters:

1. In the parameter tree, expand the **Unit > Network** node, then click **SSL**.



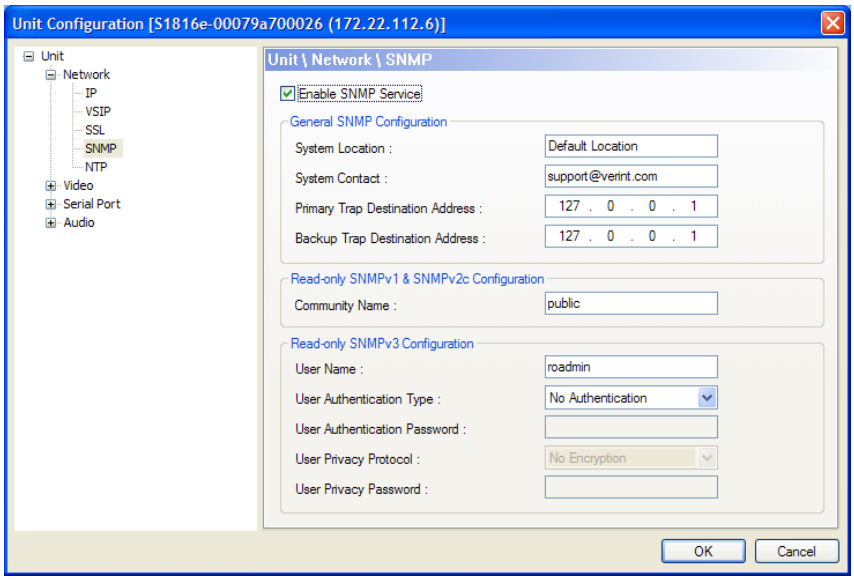
2. To change the SSL passkey:
   a. Click **Change SSL Passkey**.
      The SSL Passkey window appears.
   b. Type the passkey, then click **OK**.
3. To restrict the device to secure connections only, check **Enable Security**. After its reboot, the device will accept only SSL VSIP connections.
4. Click **OK**.

Setting the SNMP Properties

Simple Network Management Protocol (SNMP) is a protocol used by network management systems to manage network equipments from a central location. The S1800e devices are SNMP-compliant and store data about themselves in Management Information Bases (MIBs) and return this data (SNMP Traps) to the SNMP requesters.

▶ To set the SNMP parameters:

1. Double-click SConfigurator.exe to start SConfigurator.
2. Select the **Units** tab, then click **Discover**.
3. In the Units box, right-click the S1800e device, then select Batch Network Configuration to display the Batch Network Configuration dialog box.



4. In the **SNMP** panel, select the **Enabled** check box enable the SNMP service.
5. In the **System Location** box, type the location for the Edge device.
6. In the **System Contact** box, type the e-mail address of the network administrator.
7. In the **Primary Trap Destination Address** box, type the IP address of the primary server that will receive the SNMP Traps.
8. In the **Backup Trap Destination Address** box, type the IP address of the backup server that will receive the SNMP Traps in case the primary server is unavailable.
9. In the **Community Name** box, type the name of the group where you want the edge device to be a member.

NOTE: The Edge device will only respond to requests from management servers that belong to the same community.

10. In the **SNMPv3 User Name** box, type the name of the SNMP user.

11. In the **SNMPv3 User Authentication Type** list, select the authentication algorithm for SNMP requests. You can select from the following:
    - **No Authentication**

      No authentication is used.
    - **MD5 Authentication**

      The Message Digest Version 5 (MD5) hash function is used to determine that the message is from a valid source.
    - SHA Authentication

      The Secure Hash Algorithm (SHA) has function is used to determine that the message is from a valid source.
12. In the **SNMPv3 User Auth Password** box, type a password for the user.
13. In the **SNMPv3 Privacy Protocol** list, select the privacy protocol to encrypt the contents of the data. You can select from the following:
    - **No Encryption**

      No encryption is used.
    - **DES Encryption**

      The Data Encryption Standard (DES) algorithm is used to encrypt the data.
    - **AES Encryption**

      The Advanced Encryption Standard (AES) algorithm is used to encrypt the data.
14. In the **SNMPv3 Privacy Password** box, type a password for the privacy protocol.
15. Click **Apply**.
16. Click **Close**. The devices will reboot with the new configuration.

Configuring NTP

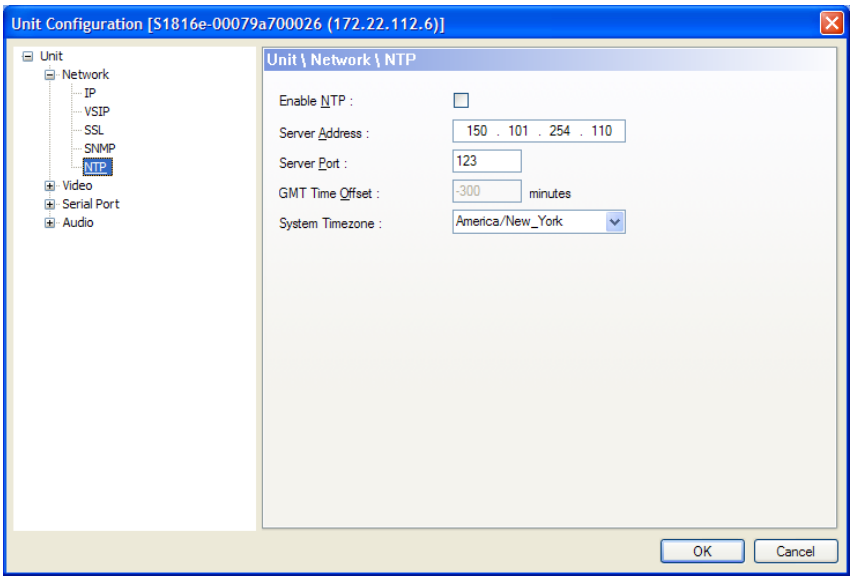
The edge device can connect to a Network Time Protocol (NTP) server to get the current time. The main reason to use NTP is to display valid dates in the log files instead of the device uptime. NTP uses GMT (Greenwich Mean Time) to synchronize device clock time.

The NTP parameters are:

- Enable NTP—The indication of whether NTP is used.
- Server Address—The IP address of the NTP server.
- Server Port—The IP port of the NTP server.
- GMT Time Offset—The offset (in minutes) from GMT in the current time zone.

▶ To change the NTP parameters:

1. In the parameter tree, expand the **Unit > Network** node, then click **NTP**.



2. Change the desired parameters.
3. Click **OK**.

Configuring Wireless

The Network>Wireless node appears only on wireless transmitters (S1100w, S1100, and S4200 series) and multipurpose outdoor wireless devices (S3100 series and S4300 series).

There are two categories of wireless parameters: communication and security.

Configuring Wireless Communication

The communication parameters are:

- Mode—The MAC (Media Access Control) mode of the device. The available values are:

MAC Mode	Description	Usage
802.11	The standard protocol for using commercial 802.11-compliant access points.	S1100w S4200e series
SDCF	The proprietary protocol optimizing the RF link by providing more data throughput. It also resolves the range and security problems of the 802.11 standard, but does not manage the hidden node issue. Starting at version 5.30, this protocol is not used anymore.	S1100 in point-to-point operations S3100 series
SPCF	The proprietary protocol that uses AES encryption (with key rotation) over the wireless link to secure communication between the devices and resolve “hidden node,” quality of service, range, and problems inherent to 802.11 wireless networking products.	S1100 in repeater contexts S1100w (default) S4200e series (default) S3100 series (default) S4300 series (default)

- Role—The function of the device in the wireless system. This parameter is not used in the 802.11 MAC mode. The available values are:

Role	Description	Usage
Master	A device that controls the access over the wireless medium. It takes care of channel selection and slave authentication to provide access to the wireless network. In the SPCF MAC protocol, the master also allocates bandwidth for all connected slaves.	S1100 S3100 series (default) S4300 series (default)
Client	A device that needs a master to access the wireless medium to transfer data. A client cannot bridge data.	S1100 S1100w (default)

Role	Description	Usage
Slave	A device that needs a master to access the wireless medium to transfer data. A slave can bridge data.	S4200 series (default) S3100 series (default) S4300 series (default)

- SSID—The service set ID used on an S1100w when the MAC mode is 802.11; it is a 2–32 character string. This value must be the same one as in the access point.
- Band—The RF (radio frequency) band used by the device. The available values are:
  - 802.11a—5 GHz OFDM
  - 802.11g—2.4 GHz OFDM
  - 4.9 GHz Public Safety—A licensed band for public safety usage in the United States, Canada, and Mexico
- Channel—The frequency channel, within the selected band, that the wireless system will use. You can perform channel selection on master devices only.
  - Master S3100 series or S4300 series—The frequency channel, within the selected band, that the wireless system will use. Two selection methods are available: manual (selecting a specific channel) or automatic (with the Auto value).
  - S1100, S1100w, S4200 series, slave S3100 series, and slave S4300 series—Even though the channel is assigned by the connected master, you can specify an initial value for the *roaming* process by which the device will find its master. However, this initial channel may not be the one used by the master.
- Channel Bandwidth—The width of the frequency channel when the 4.9 GHz public safety band is selected. The values can be 5 MHz, 10 MHz, and 20 MHz (default).

  The chosen width influences the number of available channels. For more information about channel fragmentation in the 4.9 GHz band, refer to the user guide of the wireless device.
- Bit Rate—The transmission data rate at which the device operates. This parameter is available on the S1100, S1100w, slave S3100 series, and slave S4300 series. The available bit rates vary depending on the band and channel width:

Band	Channel Width	Bit Rates (Mpbs)
2.4 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54
4.9 GHz	5 MHz	1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5
	10 MHz	3, 4.5, 6, 9, 12, 18, 24, and 27
	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54
5 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54

The Auto value is also available. It represents the best possible value (with a default RF margin of 15 dB) automatically assigned when the device connects to its master; to change the margin, see the Minimum Margin parameter. Once the device is operating properly, Verint strongly recommends to change the configured bit rate from Auto to the actual bit rate of the connection.

- Starting Order—A sequence number, used during the boot-up process of a master device in a DFS context with automatic frequency channel selection, to delay its startup. The purpose of this parameter is to ensure that colocated master devices will not start at the same time. The default starting order is 1. Every colocated cell should have a different starting order: It should be incremented by 1 in each system.
- Antenna Gain—The gain of the antenna on the device (in dBi).

  You must enter the gain if you use an external antenna with your device; with this value, the device will be able to automatically change its transmission power so that the total power (device and antenna) does not exceed the maximum value established by your country's regulations.

  With the integrated antenna on the S4200 series or S4300 series, you should also validate that the proper value for the selected RF band is displayed; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.

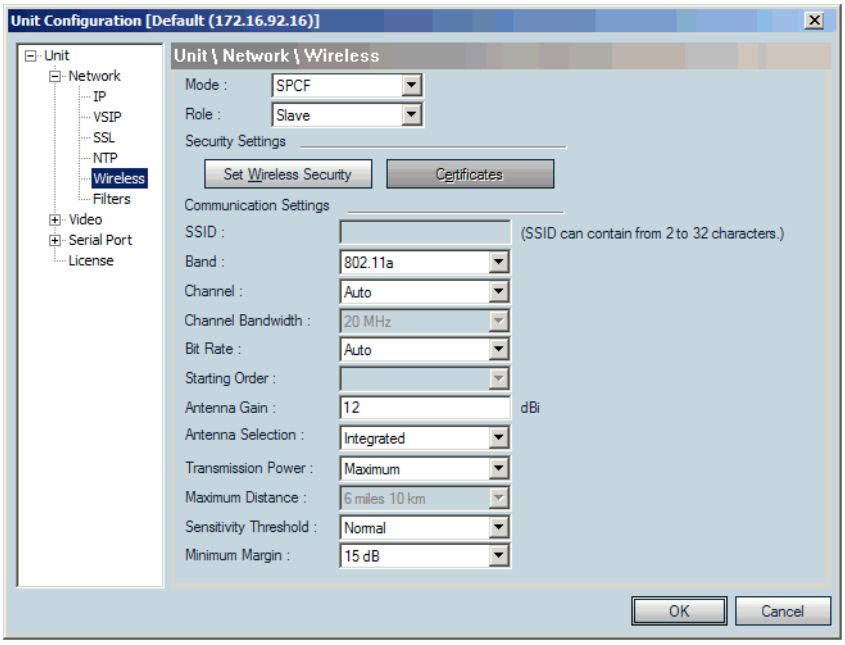
NOTE: Providing a gain lower than the gain of the antenna used by the device is strictly prohibited.

- Antenna Selection—The type of antenna that will be used on the device. The available values are:
  - Integrated—To use the antenna coming with the device.
  - External—If you installed a high gain antenna.
- Transmission Power—The indication of the level of emitting power of the device radio. The default level is the maximum allowed in your country for the configured antenna. If your system operates with a comfortable RF margin, you may reduce the emitting power to lower the noise generated on the other RF systems located nearby. The available values are:
  - Maximum—The maximum allowed.
  - 50%—The power is reduced by 3 dB.
  - 25%—The power is reduced by 6 dB.
  - 12.5%—The power is reduced by 9 dB.
- Maximum Distance—In SDCF mode, the maximum transmission distance (between a master and slave S3100 series or S4300 series) in all wireless cells present in the same geographical region and sharing the same frequency channel. The two devices making up an SDCF wireless cell must have the same value for this parameter.
- Sensitivity Threshold—The minimum signal level perceived by the radio of the device. The default value is Normal. The other available values are -80 dBm, -75 dBm, -70 dBm, and -60 dBm.

  Reducing the sensitivity of the radio enables unwanted "noise" to be filtered out. A safe value is 10 dB below the current received signal level (displayed in the Network>Wireless>Link Status node of the associated S3100 series or S4300 series). The default value represents the most sensitive context. You must be careful not to reduce the sensitivity to a level where the device would not "hear" its legitimate correspondent.
- Minimum Margin—The minimum RF margin used when the transmission bit rate is set to Auto. It represents the difference in dB between the actual signal received by the device and the minimum signal required by a given bit rate to correctly receive data on the RF link. The default minimum margin is 15 dB. This parameter is available on the client and slave devices.

To change the wireless parameters for an S1100w, S1100, or S4200 series:

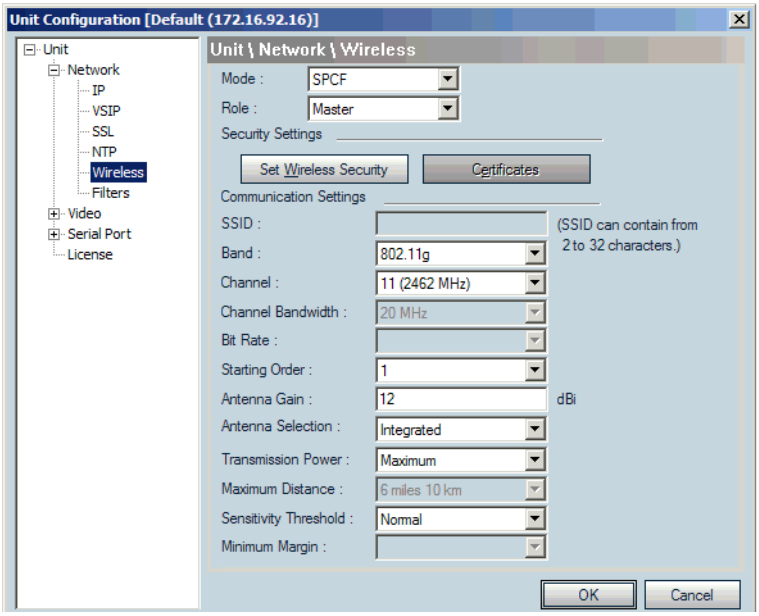
1. In the parameter tree, expand the **Unit > Network** node, then click **Wireless**.



2. Change the parameters as required.
3. Click **OK**.

To set the wireless parameters for a master S3100 series or S4300 series:

1. In the parameter tree, expand the **Unit > Network** node, then click **Wireless**.



2. Ensure that the **Role** box contains **Master**.
3. In SDCF mode, set the value of the **Maximum Distance** box.
4. Change the other parameters as required.
5. Click **OK**.

▶ To set the wireless parameters for a slave S3100 series or S4300 series:

1. In the parameter tree, expand the **Unit > Network** node, then click **Wireless**.
2. In the **Role** box, select **Slave**.
3. Change the other parameters as required.
4. Click **OK**.

Configuring Wireless Security

Security is very important on a wireless network. Security mechanisms must be put in place to avoid eavesdropping and attacks on the network. The available security parameters vary depending on the MAC mode (SPCF, SDCF, or 802.11) of the wireless device.

All security mechanisms use a key to enable secure and encrypted RF communication between wireless devices. This user-supplied key is case sensitive. For the wireless connection to be secure, do no enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the key.

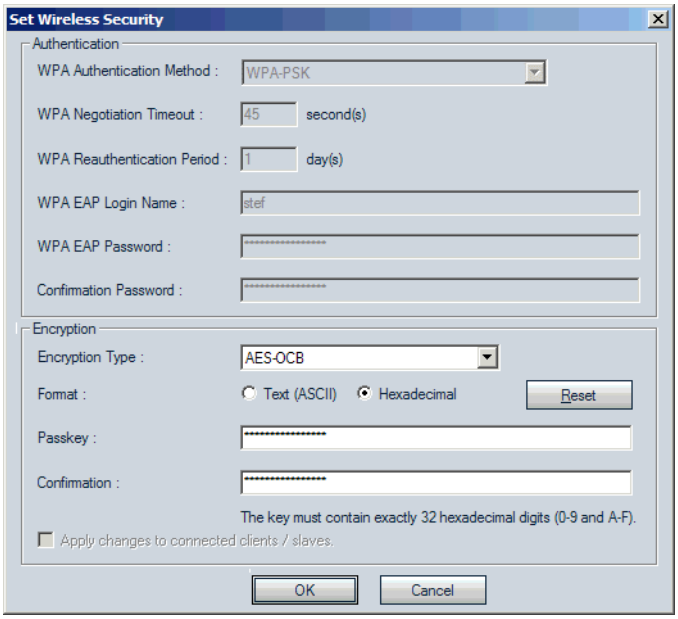
SPCF and SDCF

In SPCF and SDCF, the wireless devices use a wireless passkey with the AES-OCB encryption and automatic key rotation. Security is always activated.

▶ To change the wireless passkey in SPCF or SDCF:

NOTE: To change security parameters, you need a secure VSIP SSL connection between the device and SConfigurator; for the procedure, see *Chapter 4: Enabling Security*.

1. In the parameter tree, expand the **Unit > Network** node, then click **Wireless**.



2. In the **Format** list, select the format of the passkey: **Text (ASCII)** or **Hexadecimal**.
3. In the **Passkey** box, enter the new passkey (case-sensitive). The user-supplied passkey must be unique and have exactly 16 characters if the format is Text, or 32 digits if Hexadecimal.
4. In the **Confirmation** box, enter again the passkey.
5. To set the wireless passkey to its default value, click **Reset**.
6. **OK**.

802.11

You can use the 802.11 MAC mode with the S1100w and S4200 series only. The parameter values must be the same as those entered in the commercial 802.11 access point.

In 802.11, the following security mechanisms are available:

- No security—Not recommended
- WEP—Not recommended
- WPA and WPA2 (also known as *802.11i*) in personal mode (PSK)
- WPA and WPA2 in Enterprise mode, with an 802.1X authentication server

The supported 802.11 authentication methods are:

Authentication Method	Authentication Means	Remarks
PSK—pre-shared key (personal)	passphrase	A passphrase is required to connect to an access point and therefore access the network.
EAP-TLS (Enterprise)	certificate	Uses mutual authentication. The most secure option available.
EAP-TTLS (Enterprise)	login/password and certificate	Creates a secure TLS tunnel. Supports MSCHAPv2 (the Microsoft version of the Challenge Handshake Authentication protocol) to validate logins and passwords. A certificate is required on the server side.
EAP-PEAP (Enterprise)	login/password and certificate	Creates a secure TLS tunnel. Supports MSCHAPv2 (the Microsoft version of the Challenge Handshake Authentication protocol) to validate logins and passwords. A certificate is required on the server side.

For more information about the TLS protocol, refer to RFC 2246 at http://www.ietf.org/rfc/rfc2246.txt.

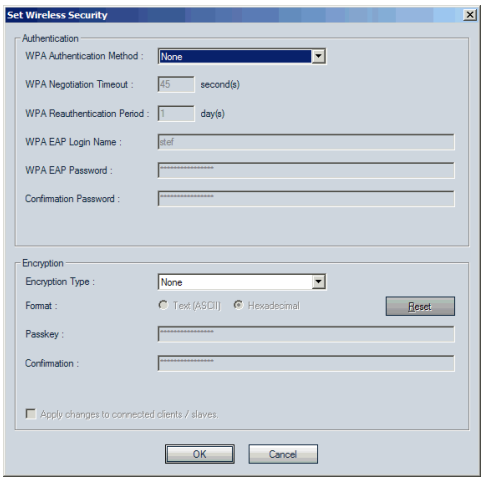
The supported encryption methods for 802.11 are:

- WEP
- AES-CCMP
- TKIP
- Auto-select—The device automatically chooses the best available encryption scheme.

▶ To specify the authentication method and the wireless key in the 802.11 mode:

NOTE: To change security parameters, you need a secure VSIP SSL connection between the device and SConfigurator; for the procedure, see *Chapter 4: Enabling Security*.

1. In the parameter tree, expand the **Unit > Network** node, then click **Wireless**.
2. Click **Set Wireless Security**. The Set Wireless Security window appears.



3. In the **WPA Authentication Method** list, select the desired authentication method.
4. In the **WPA Negotiation Timeout** list, enter the maximum time (in seconds) given for the device to be authenticated.
5. If a WPA2 authentication method was selected, enter the frequency (in days) at which the authentication process will be re-activated with new keys in the **WPA Reauthentication Period** box. This re-authentication process is transparent and will not affect video. It increases security and helps prevent eavesdropping.
6. If a TTLS or PEAP authentication method was selected:
   a. In the **WPA EAP Login Name** box, enter a login name (case-sensitive). The login name must contain between 0 and 63 characters.
   b. In the **WPA EAP Password** box, enter a password (case-sensitive). The password must contain between 0 and 63 characters.
   c. In the **Confirmation Password** box, enter again the password.
7. In the **Encryption Type** list, select the desired encryption algorithm.

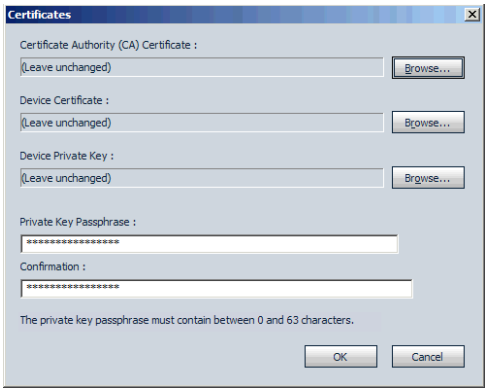
NOTE: The available encryption types vary depending on the authentication method.

8. If the encryption type is one of the WEP flavors, select the format of the key: **Text (ASCII)** or **Hexadecimal**.
9. In the **Passphrase** or **Passkey** box, enter the new encryption key (case-sensitive).
10. In the **Confirmation** box, enter again the key.
11. To set the key to its default value, click **Reset**.
12. Click **OK**.

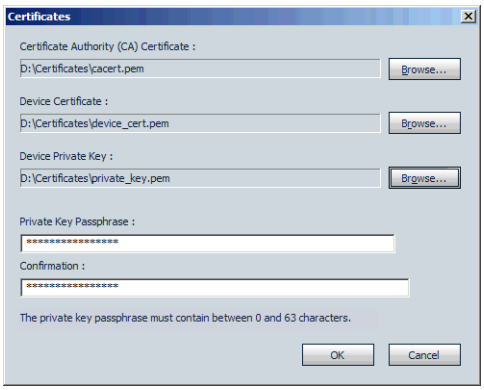
▶ To set an 802.11 certificate for EAP-TLS, EAP-TTLS, or EAP-PEAP:

NOTE: To change security parameters, you need a secure VSIP SSL connection between the device and SConfigurator; for the procedure, see *Chapter 4: Enabling Security*.

1. In the parameter tree, expand the **Unit > Network** node, then click **Wireless**.
2. Click **Certificates**.



3. In the **Certificate Authority (CA) Certificate** box, click **Browse**, then select the file holding the certificate provided by the CA. Typically it is a `.pem` file.
4. In the **Device Certificate** box, click **Browse**, then select the file holding the device certificate. Typically it is a `.pem` file.
5. In the **Device Private Key** box, click **Browse**, then select the file holding the private key of the device. Typically it is a `.pem` file.



6. In the **Private Key Passphrase** box, enter the passphrase associated to the certificate (case-sensitive). The passphrase must contain between 0 and 63 characters.
7. In the **Confirmation** box, enter again the passphrase.
8. Click **OK**.

Accessing the Link Status

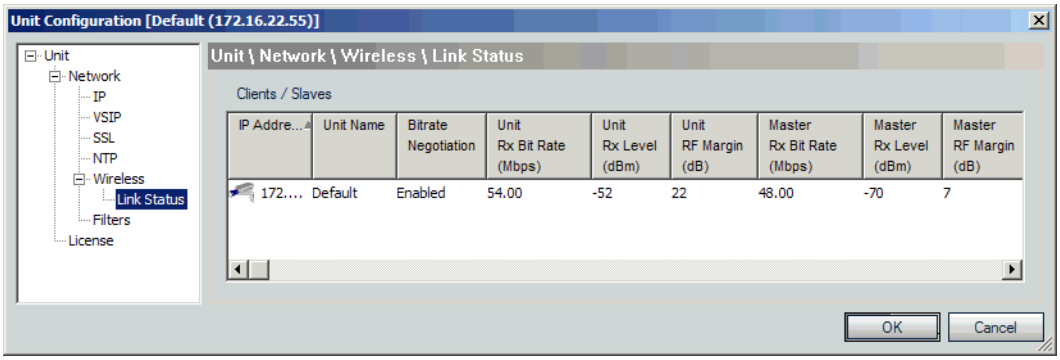
The Network>Wireless>Link Status node status contains information on the devices (client or slave) connected to a master S3100 series or S4300 series:

- IP Address—The IP address of the device.
- Unit Name—The name of the device.
- Bitrate Negotiation—The indication of whether there is negotiation for the bit rate between the devices. This parameter is set by the RF protocol; it is always Enabled.
- Unit Rx Bit Rate—The reception data rate (in Mbps) of the client or slave. It corresponds to the transmission bit rate of the master.
- Unit Rx Level—The average signal level (in dBm) indicating the strength of the signal received by the client or slave.
- Unit RF Margin—The RF margin (in dB) used by the client or slave.
- Master Rx Bit Rate—The reception data rate (in Mbps) of the master. It corresponds to the transmission bit rate of the client or slave. You can manually change this value.
- Master Rx Level—The average signal level (in dBm) indicating the strength of the signal received by the master.
- Master RF Margin—The RF margin (in dB) used by the master.

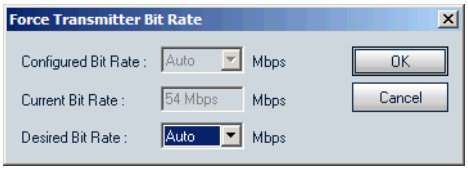
Once a client or slave device is operating properly, Verint strongly recommends to change its configured bit rate from the default value to the actual bit rate of the connection. This way, the wireless communication will be more stable in the presence of changing atmospheric conditions or other RF interferers. If the quality of the RF link degrades severely, the actual bit rate could be lower than the manually configured one.

▶ To change the transmission bit rate of a client or slave:

1. In the parameter tree of the master device, expand the **Unit > Network** > **Wireless** node, then click **Link Status**.



2. In the **Clients/Slaves** list, right-click the desired device, then select **Force Transmission Bit Rate**.



3. In the **Desired Bit Rate** box, select the new value, then click **OK**. The device reboots. The new bit rate is then displayed in the list.

NOTE: To change the bit rate of the same device a second time, you need to leave the Unit Configuration window, re-discover the devices, then access the configuration parameters of the master.

Selecting Multicast Filters

The Network>Filters node contains the parameters for controlling the flow of data between the wireless and wired Ethernet networks in a multicast environment. These parameters are not taken into account for broadcast communication. This node appears on wireless devices only.

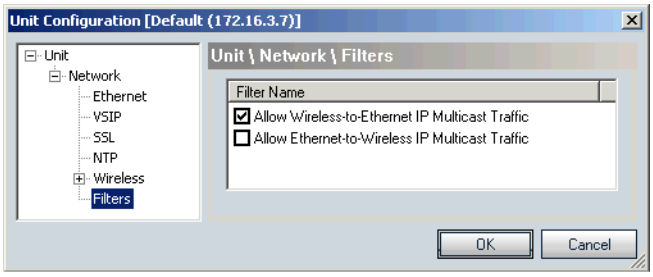
The available filters allowing multicast traffic are:

- From the wireless to the wired network
- From the wired to the wireless network

By default, wireless-to-wired traffic is enabled, allowing data to flow from wireless transmitters to the wired network (either Verint video receivers or computers running a video management software).

▶ To select multicast filters:

1. In the parameter tree, expand the **Unit > Network** node, then click **Filters**.



2. Select the desired filters.
3. Click **OK**.

Configuring Video

The Video node in the parameter tree enables you to properly configure video on transmitter and receiver devices. You can change:

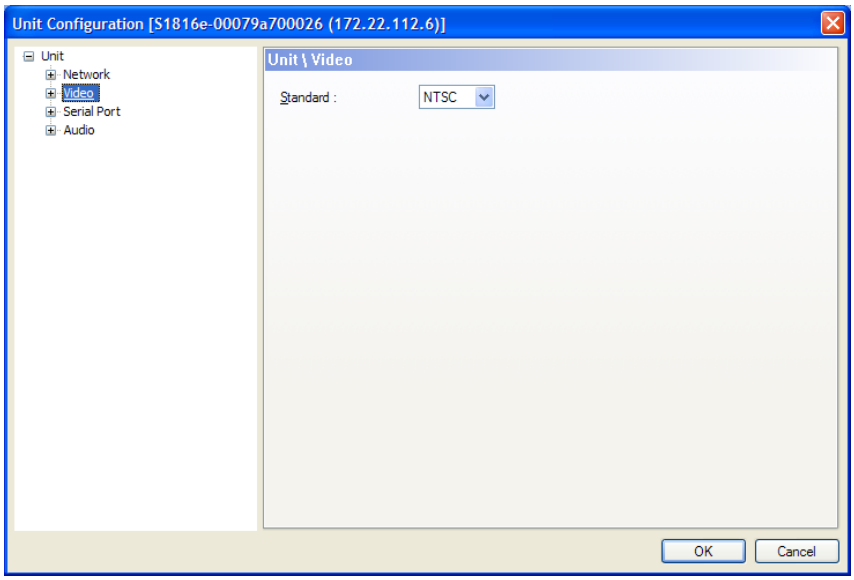
- The video standard
- The treatment of color on each video input
- The encoders
- The brightness of each video output

Configuring the Video Standard

You can change the analog display standard.

▶ To change the video standard:

1. In the parameter tree, expand the **Unit > Video** node.



2. In the **Standard** list, select the analog display standard. Possible values are:
   - NTSC—Used in North America, Central America, a number of South American countries, and some Asian countries, including Japan.
   - PAL—Used in United Kingdom, much of western Europe, several South American countries, some Middle East and Asian countries, several African countries, Australia, New Zealand, and other Pacific island countries.
3. Click **OK**.

Configuring the Treatment of Color on an Input

A series of parameters relative to the treatment of colors is available for each video input:

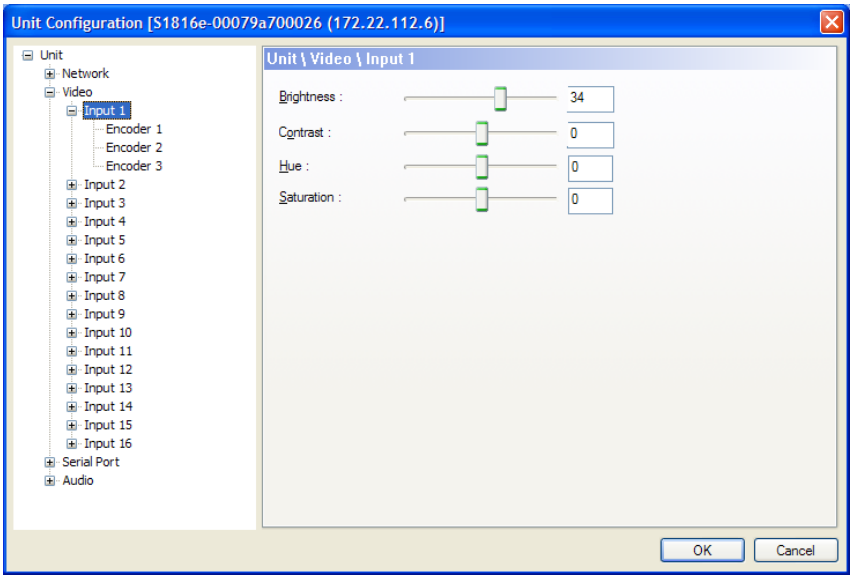
NOTE: These parameters are not available on the S2500e and S2600e series IP cameras.

- Brightness—The total amount of light in a color. The values range from -128 (no brightness) to 127 (white).
- Contrast—The range of colors in the image. The values range from -128 (luminance off) to 127; 0 is the CCIR level. Increasing the contrast of a color palette makes different colors easier to distinguish, while reducing the contrast makes them appear washed out.
- Hue—The relative amounts of red, green, and blue in a color. The values range from -180 (-180d) to 179 (179d); 0 is 0d. Hue corresponds to the common definition of color; for example, "red," “orange,” and “violet.”
- Saturation—The vividness of a color, the intensity of the colors in the image. The values range from -128 (color off) to 127; 0 is the CCIR level.

The number of video inputs varies depending on the transmitter device.

▶ To change the video input parameters:

1. In the parameter tree, expand the **Unit > Video** node, then click the desired **Input**.



2. Change the desired parameters.
3. Click **OK**.

Configuring an Encoder

You can configure the parameters of each encoder of a video input. Most devices support dual encoding, that is, the sending of the incoming video to two separate encoders; in such a context, you can customize each encoder to meet your system needs, for instance in terms of frame rate and resolution. Dual encoding requires more bandwidth.

The number of encoders varies depending on the product:

Product	Number of Encoders
S1100w	One encoder for the single input (typical); to enable the second video encoder, call customer service.
S1704e, S1704e-AS, S1708e, S1708e-AS, S1712e	Two encoders per input (dual encoding)
S1724e	One encoder per input (single encoding)
S1800e Series - Mulitport	Three encoders per input (triple encoding)
S1800e Series - Single/ Dual ports	Four encoders per input (quad encoding)
S1900e series	Two encoders on the single input (dual encoding)
S1900e-Vicon	Two encoders on the single input (dual encoding)
S2500e	Two encoders on the single input (dual encoding)
S2600e series	Two encoders on the single input (dual encoding)
S2700e series	Two encoders on the single input (dual encoding)
S2750e series	Two encoders on the single input (dual encoding)
S4200	Two encoders on the single input (dual encoding)
S4200-AS	Two encoders on the single input (dual encoding)
S4200-2V	One encoder per input (single encoding)
S4200-AS-2V	Two encoders per input (dual encoding)

You can change the following parameters:

- Target Bit Rate—The maximum number of bits per second that you want the device to generate. Valid bit rates range from 9 to 6000 kbps. This value depends on many variables, like network capacity and the number of devices sending data on the network.
- Target Frame Rate—The maximum number of frames per seconds (fps) that will be encoded and transferred by the transmitter. This parameter can be set to 1 to 7, 10, 15, or 30 fps in NTSC mode and 1 to 6, 8, 12, or 25 fps in PAL mode.
- Minimum Quantizer—The high video quality boundary. The lower the value, the higher the video quality and the file size. The available values are in the 2–31 range.

- Maximum Quantizer—The low video quality boundary. A higher quantizer value means less video quality but a smaller file size. To maintain the video frame rate (that is, not to skip any frames), you should set the maximum quantizer to 31. If the quality of each frame is more important, you should reduce the quantizer value; for example, a maximum quantizer of 5 keeps a good image quality, but skips frames when motion is high. The available values are in the 2–31 range.
- Intra Interval—The frequency at which a complete video frame (called *I-frame*) is sent by the encoder. The available values are in the 0–1000 range. A value of 0 indicates that no I-frame will be sent automatically by the device; a value of X means that a complete image refresh will occur every X frames.
- Rate Control—The mode controlling the bit rate variation. The available modes are:
  - Constant Frame Rate—This mode maintains the target frame rate. Video quality may suffer and the bit rate may exceed the target value.
  - Constant Bit Rate—This mode is the most effective to maintain the target bit rate. Video quality may suffer (frames may be skipped) and the frame rate may decrease. This mode should be used when transmitting video over networks that have very limited bandwidths, and with an intra interval value of 0 (default).
  - Constant Storage Rate—This is the optimized mode to be used only for the Nextiva video management software.
  - Advanced Constant Bit Rate—This mode maintains the target bit rate but is less precise than the constant bit rate. Video quality may suffer and the frame rate may decrease. This mode is preferred for high frame rate contexts.

NOTE: This mode is available only on the S1100w.

- Resolution—The measure of how clear and crisp the video image appears. Each resolution corresponds to a specific number of pixels (columns * lines) for each picture of the video sequence. A high resolution increases picture quality but at the price of raising the bit rate. For example, the 2CIF and 4CIF modes should not be used with a bandwidth of less than 1000 kbps.

  The available resolutions are:

Resolution	Number of Columns	Number of Lines		Availability
	NTSC/ PAL	NTSC	PAL	
QCIF	176	128	144	All devices except the multiport S1700e and S1800e series.
CIF	352	240	288	All devices
2CIF	704	240	288	All devices
4CIF	704	480	576	All devices
All lines	352	480	576	All devices except the multiport S1800e series.

Resolution	Number of Columns	Number of Lines		Availability
	NTSC/ PAL	NTSC	PAL	
2/3D1	480	480	576	All devices except the multiport S1800e series.
VGA	640	480	480	All devices except the multiport S1800e series.

- Input Filter—The level of filtering applied to the video signal before it is encoded, helping to remove high frequency noise from lower quality cameras or noisy video feeds. The available values are Low, Medium, High, or None.

NOTE: This option is not available for the multiport S1800e series.

In removing noise from the video signal, the filter also reduces the sharpness of the image. If the signal is relatively clean, use a parameter of None to avoid losing crispness. For images with too much noise, applying the filter can help clean up the image. Keep in mind however that the higher the filter level, the blurrier the video image may become.

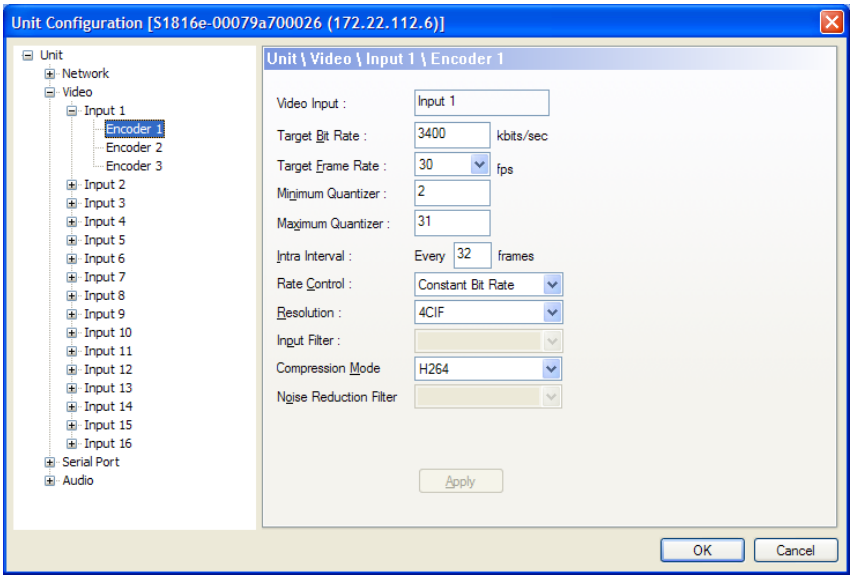
- Compression Mode—The way video is compressed. The following modes are available:
  - SM4—The proprietary MPEG-4-based mode.
  - MPEG4—The MPEG-4 ISO 14496-2 compliant mode. This mode is available on all devices except the S1100w.
  - H.264—The MPEG-4 Part 10 (MPEG-4 AVC) ISO 14496-10 compliant mode. This mode is only available on the multiport S1800e series.
- Noise Reduction Filter—The filtering of small variations in pixels in otherwise motionless sections of the video, to be used in all conditions to reduce the bit rate. Using this filter also helps reduce the number of false alarms in low light conditions. The available values are Low (default), Medium, High, and None.

NOTE: This option is not available for the multiport S1800e series.

On the S1900e-Vicon, S1950e, S2600e, S2610e, S2700e series, and S2750e series devices, you need to deactivate the second encoder for that setting to take effect. To do this, go in the web interface, select the Advanced > Video page, then change the value of the Number of Encoders per Video Input parameter to 1. Finally, save the settings and reboot the device.

To change the video encoder parameters:

1. In the parameter tree, expand the **Unit > Video** > **Input x** nodes, then click the desired **Encoder**.



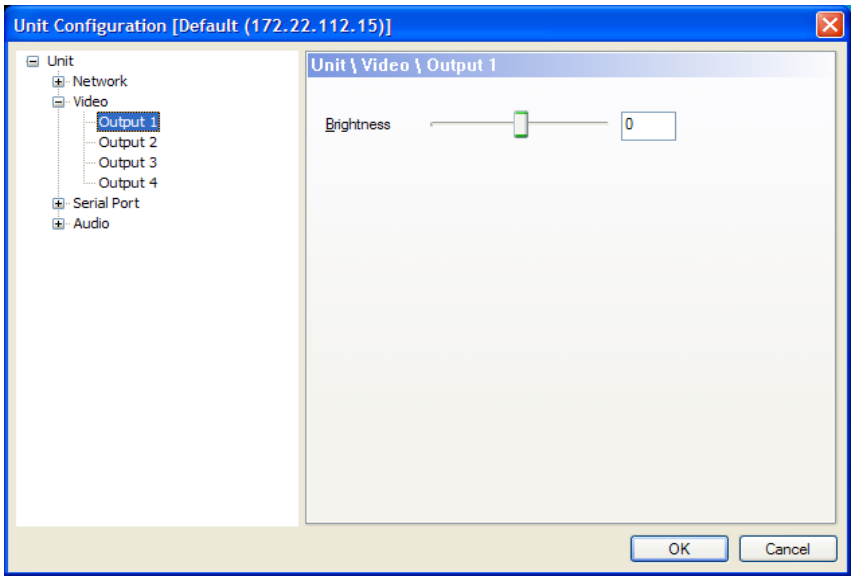
2. Change the desired parameters.
3. In a point-to-point context, to immediately see the changes on the analog monitor (except for **Rate Control** and **Resolution**) without saving them, click **Apply**.
4. Click **OK**.

Configuring the Brightness of a Receiver

You can configure the brightness (total amount of light in a color) on each video output of a receiver. The number of video outputs varies depending on the device.

▶ To change the video decoder parameter:

1. In the parameter tree, expand the **Unit > Video** node, then click the desired **Output**.



2. If required, change the brightness.
3. Click **OK**.

Configuring the Serial Port

The Serial Port node in the parameter tree allows you to specify how the device will communicate with the serial equipment (PTZ camera, keyboard, matrix, multiplexer, or access card). Not all devices have a serial port.

The number and types of serial ports vary depending on the device:

Device	Number of Serial Ports	Type of Serial Port
S1100w	1	Either RS-232 or RS-422/485 (auto-detected)
S1504e-R	2	RS-232 and RS-422/485 ports
Multiport S1700e series	2	RS-232 and RS-422/485 ports
Multiport S1800e series	2	RS-232 and RS-422/485 ports
Single.Dual port S1800e series	1	RS-232 orRS-422/485 ports
S1900e series	1	RS-422/485
S4200 series	1	RS-422/485

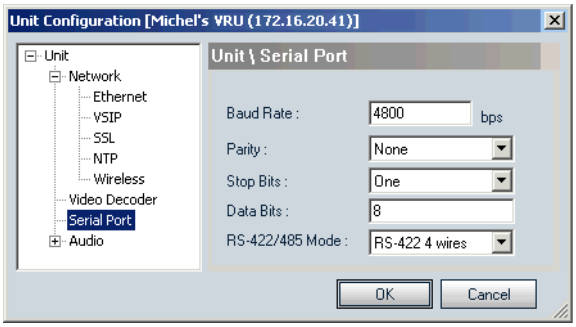
The serial port parameters are:

- Baud Rate—The data rate that the serial equipment operates at. Possible values range from 1200 bps to 230,400 bps (transmitters) or to 115,200 bps (receivers).
- Parity—Odd, even, or no parity check. Most communication devices do not use parity.
- Stop Bits—The number of stop bits in each transmission.
- Data Bits—The number of bits in transmitted data.
- RS-422/485 Mode—The way the RS-422/485 serial equipment will interface with the Verint device. The supported operating modes are: RS-422 4 wires, RS-485 2 wires, and RS-485 4 wires. This parameter only applies to an RS-422/485 port.

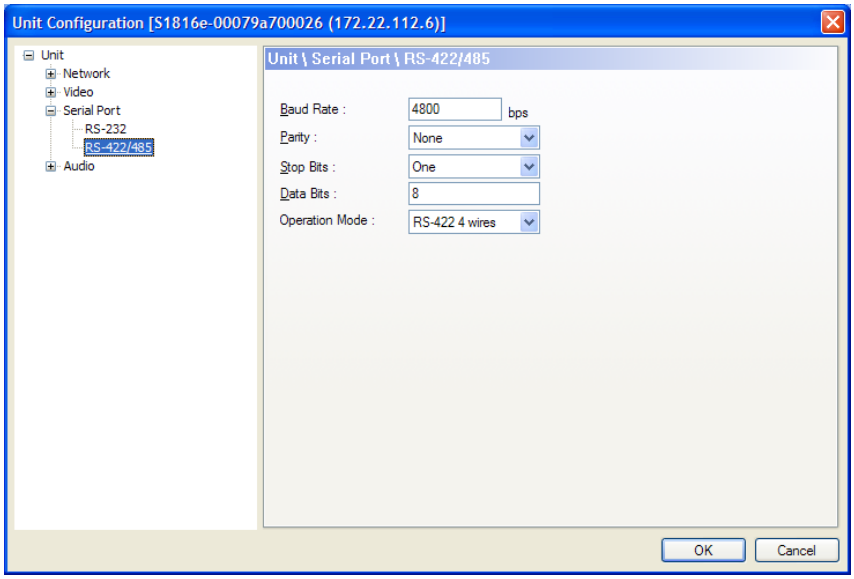
For more information about these parameters, refer to the serial equipment documentation or contact your product manufacturer.

To change the serial port parameters:

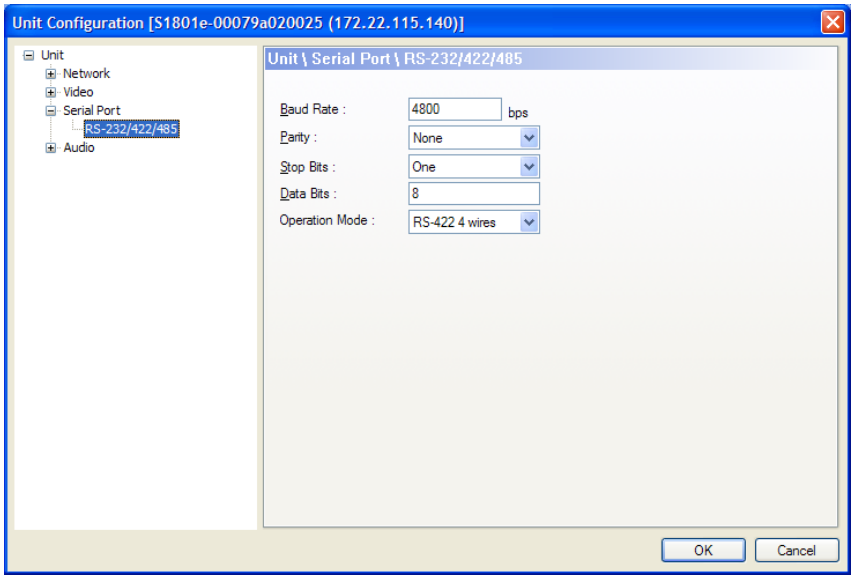
1. For an S1100w device, expand the **Unit > Serial Port** node in the parameter tree.



2. For the other device, expand the **Unit > Serial Port** node, then click the desired serial port.



   - For the Single/Dual port S1800e encoders, select RS4232/422/485.



3. Change the desired parameters.
4. Click **OK**.

Configuring Audio

The Audio node in the parameter tree enables you to properly configure the audio on transmitter or receiver devices. It appears in the parameter tree only if audio is supported on your edge device. The number of audio encoders (or *audio inputs*) and decoders (*audio outputs*) varies depending on the device.

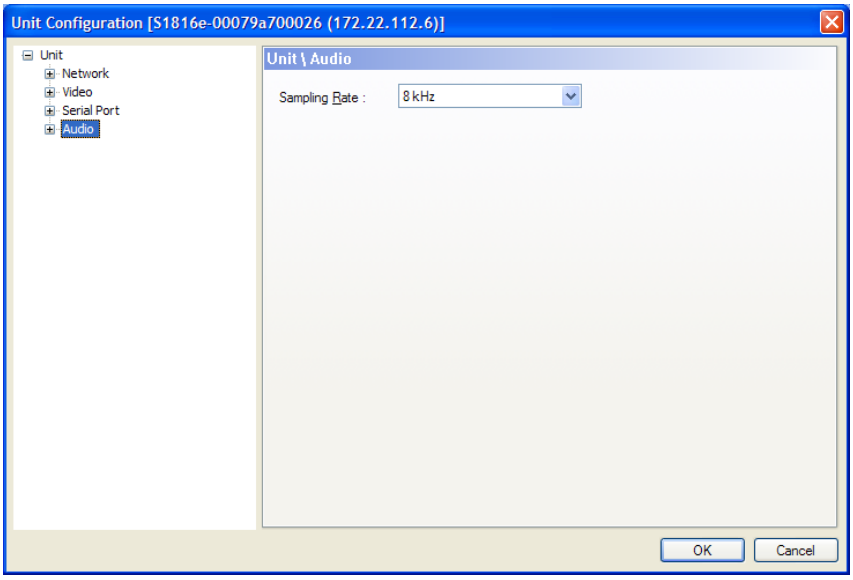
To enable the audio functions in a point-to-point connection, see *page 63*. For details about the required physical connections for audio, refer to the user guide of your device.

Configuring the Sampling Rate

The sampling rate represents the rate (in kHz) at which the samples of the analog audio signal are taken in order to be converted into digital form. The available rates are: 8 kHz, 16 kHz, or 24 kHz. This parameter applies to the S1708e and S1712e with 12 audio inputs only.

▶ To change the sampling rate:

1. In the parameter tree, expand the **Unit > Audio** node.



2. In the **Sampling Rate** box, select a new value.
3. Click **OK**.

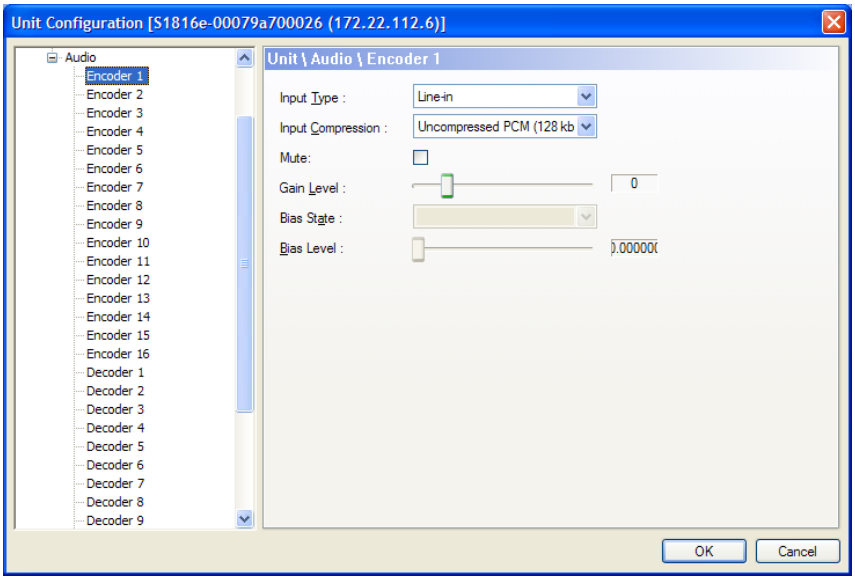
Configuring an Audio Encoder

The audio encoder parameters are:

- Input Type—The type of your audio source. Depending on the product, the following modes may be available:
  - Line-in—The audio is not amplified: it needs a pre-amplifier; for example, a CD reader.
  - Mic (with pre-amp)—The audio does not need to be amplified; for example, an intercom.
- Input Compression—The transfer mode for audio data. You select your mode depending on your bandwidth and the desired audio quality. The following modes are available depending on your device:
  - Uncompressed PCM (128 kbps)—There is no compression. Audio quality is the best, at the expense of the bandwidth.
  - ULAW (64 kbps)—A North American standard for converting analog data into digital form using pulse code modulation (PCM) (default).
  - GSM (13 kbps)—The first mobile phone standard. Since there is a lot of compression, audio quality may suffer.
- Gain State—The indication of whether audio is amplified. Setting it to Disabled corresponds to mute. This parameter applies to the S1708e and S1712e with 12 audio inputs only.
- Gain Level—The amplification level. The level is taken into account only when the gain is enabled. This parameter applies to the S1708e and S1712e with 12 audio inputs only.
- Bias State—The indication of whether the bias is enabled on the device. This parameter applies to the S1708e and S1712e with 12 audio inputs only.
- Bias Level—The level of voltage applied to a microphone to set its condition of operation. The bias level is taken into account only when the bias is enabled. The available values are in the 0–9 volt range. This parameter applies to the S1708e and S1712e with 12 audio inputs only.

▶ To change the audio encoder parameters:

1. In the parameter tree, expand the **Unit > Audio** node, then click the desired **Encoder**.



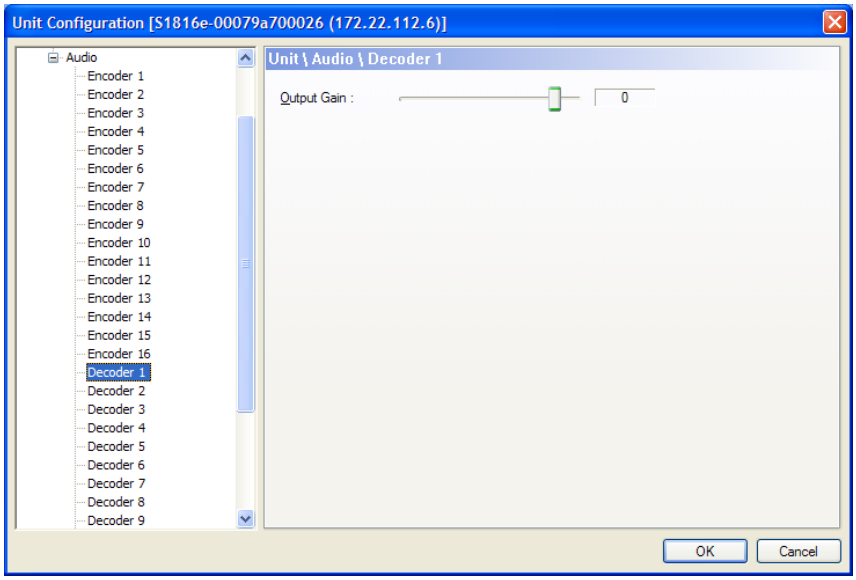
2. Change the desired parameters.
3. Click **OK**.

Configuring an Audio Decoder

The only audio decoder parameter is the output gain that represents the amplification level.

▶ To change the output gain:

1. In the parameter tree, expand the **Unit > Audio** node, then click **Decoder**.



2. Change the output gain by moving the slider either to the right to increase the volume, or to the left to lower it.
3. Click **OK**.

Configuring the S4100 Series

The S4100 series is a professional video transmission product designed for the CCTV (closed circuit television) market. It consists of a video encoder/transmitter (-T) and a video decoder/receiver (-R) device. This product leaves the Verint factory with preset IP network parameters that cannot be modified.

The steps to configure this product are:

1. Preparing the devices for configuration
2. Assigning initial parameters
3. Performing an advanced configuration (if required)
4. Resetting the configuration

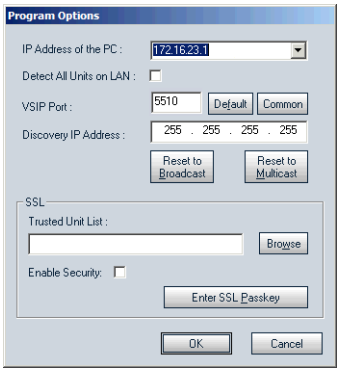
Preparing the Configuration

Because the network configuration of the S4100 series is pre-assigned, you need to temporarily change the IP address of the computer running SConfigurator to be able to reach the devices. For more information, refer to the Verint *S4100 Series User Guide*.

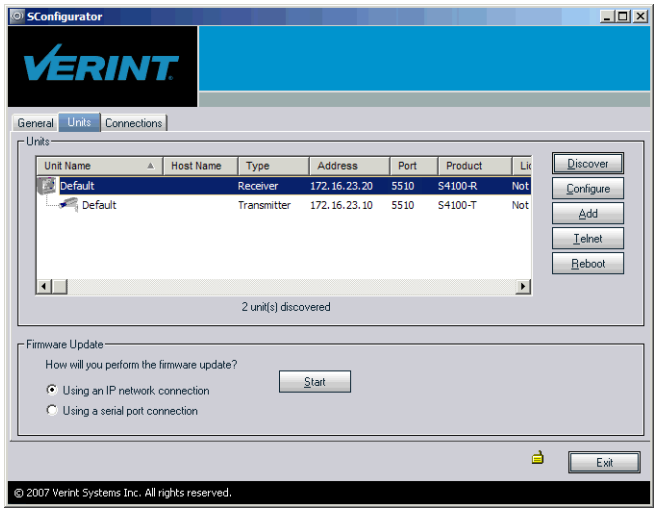
▶ To prepare the configuration of the S4100 pair:

1. Change the IP address of the computer running SConfigurator; the recommended temporary IP parameters are:
   - IP address: 172.16.23.01
   - Subnet mask: 255.255.0.0
   - Default gateway: 172.16.23.1

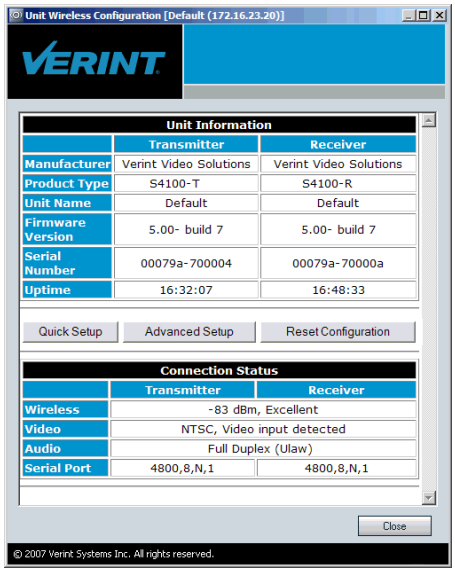
   Write down the initial state of the computer to revert to these values after the configuration is finished.
2. Power the S4100-R and establish its Ethernet connection.
3. Power the S4100-T.
4. Start SConfigurator.
5. In the General tab, click **Program Options**. The Program Options window appears.



6. In the **IP Address of the PC** list, select **172.16.23.1**. If it does not appear in the list, it may be because you did not temporarily change the IP address of your computer.
7. Ensure that the **VSIP Port** is 5510; otherwise, click **Default**.
8. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.
9. Click **OK**.
10. Select the **Units** tab, then click **Discover**. The two devices appear in the Units list.



11. Select the device, then click **Configure**. The Unit Wireless Configuration window appears.



12. Click **Quick Setup**.

Assigning Initial Parameters

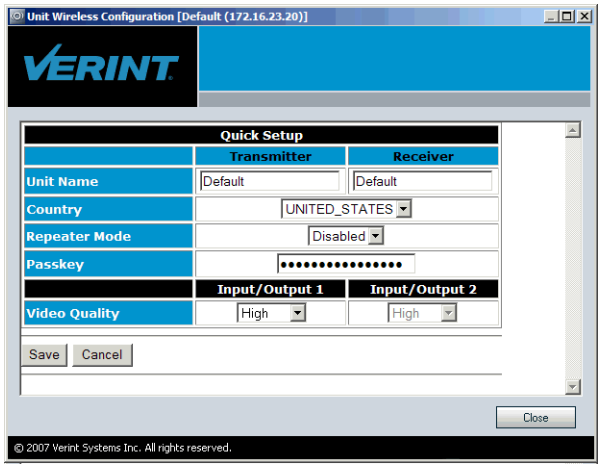
You can easily set up your radio system by providing a minimal set of parameters. The parameters vary depending on your application (point-to-point system or point-to-point repeater).

When selecting the video quality of the device, it is recommended to use one of the following five preset video qualities:

Parameters	Very High	High	Medium	Low	Very Low
Resolution	4CIF	All lines	CIF	CIF	CIF
Frame rate in NTSC/ PAL (frames per second)	30/25	30/25	30/25	7/6	4/3
Bit rate (kbps)	3000	2046	1024	512	256
Min. quantizer	2	2	2	2	2
Max. quantizer	15	15	15	15	15
Input filter	None	Low	Low	Low	Low
Deblocking filter	On	On	On	On	On

▶ To set the parameters for a point-to-point system:

1. In the **Unit Name** boxes of the Quick Setup window, provide a meaningful name for the devices.



2. In the **Country** box, select the country of operation of the pair of devices. Assign the proper country to comply to the DFS/TPC regulations, if applicable, to respect the maximum EIRP, and to use the proper set of frequency channels.
3. Ensure that the **Repeater Mode** value is **Disabled**.
4. In the **Passkey** box, enter the wireless passkey common to the transmitter and receiver. This user-supplied passkey is case sensitive and must have exactly 16 characters.

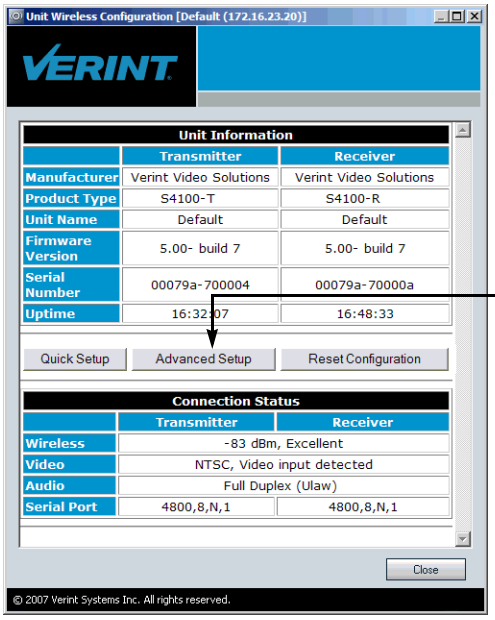
5. In the **Video Quality** box (two boxes are available for a -2V product), select the desired video quality. The following preset values are available: Very Low, Low, Medium, High, and Very High.
6. Click **Save**. The receives its configuration through the wireless network. The devices reboot.
7. In the Unit Wireless Configuration window, click **Close**.
8. In the SConfigurator window, click **Exit**.
9. Unplug the Ethernet cable from the device, then put back the dust cap on the network (RJ-45) connector.
10. Connect the monitor and camera to the devices; ensure that RF and video communication works properly in your wireless system.

▶ To set the parameters for a point-to-point repeater system:

1. In the **Unit Name** boxes of the Quick Setup window, provide a meaningful name to the two devices.
2. In the **Country** box, select the country of operation of the pair of devices. Assign the proper country to comply to the DFS/TPC regulations, if applicable, to respect the maximum EIRP, and to use the proper set of frequency channels.
3. In the **Repeater Mode** box, select **Enabled**.
4. In the **Passkey** box, enter two different passkeys, one per wireless cell. These user-supplied passkeys are case sensitive and must have exactly 16 characters.
5. In the **Video Quality** box (two boxes are available for a -2V product), select the desired video quality.
6. Click **Save**. As soon as these settings are saved, the devices are not communicating anymore, since they have different wireless passkeys. The RF and video communication will be re-established after the repeater is fully configured. The receives its configuration through the wireless network. The devices reboot.
7. In the Unit Wireless Configuration window, click **Close**.
8. In the SConfigurator window, click **Exit**.
9. Unplug the Ethernet cable from the device, then put back the dust cap on the network (RJ-45) connector.
10. Configure the two S4300 devices making up the repeater. For the procedure, refer to the Verint *S4300-RP Installation Guide*.
11. Connect the monitor and camera to the devices; ensure that RF and video communication works properly in your wireless system.

Performing an Advanced Configuration

In addition to the Quick Setup window in SConfigurator, you have access to a more elaborate set of parameters (general, wireless, video, audio, and serial port). You can use them to fine tune the configuration of your devices (for instance if you are collocating many systems) or to troubleshoot your devices with a customer service specialist.



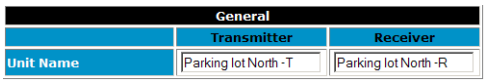
Also, the Connection Status area provides the current state of the device pair:

- Wireless: the signal level and the communication quality
- Video: the video format and the state of the video signal
- Audio: the state of the audio signal
- Serial Port: the bit rate, number of data bits, parity, and number of stop bits

You can change the names of the devices.

▶ To change the general parameter of the devices:

1. In the Unit Wireless Configuration window in SConfigurator, click **Advanced Setup**.
2. Locate the **General** area.



3. In the **Unit Name** boxes, enter meaningful names for the devices.
4. If you are finished with the changes, scroll down the window, then click **Save**. The devices reboot.

The available wireless parameters are:

- Country—The country of operation of the devices.

  You must assign the proper country to comply to the DFS/TPC regulations if applicable, to respect the maximum EIRP, and to use the proper set of frequency channels.
- Repeater Mode—The indication of whether the is part of a point-to-point repeater system.

- Passkey—A unique, 16 character, case-sensitive identifier enabling secure and encrypted RF communication between the two wireless devices:
  - If the devices form a point-to-point system, enter the passkey common to the transmitter and receiver.
  - If the devices are in repeater mode, enter two different passkeys.

  For the wireless connection to be secure, do no enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.
- Pair Number—A unique number to assign to the devices when more than one pair are used with the same S4300-RP repeater.
- RF Band—The frequency band used by the device. The available values are:
  - 802.11a (5 GHz OFDM)
  - 802.11g (2.4 GHz OFDM)
  - public safety 4.9 GHz
- Channel—The RF channel used by the device. You can either manually select the channel or use the automatic channel selection (default).
- Channel Bandwidth—The width of the frequency channel; this parameter only applies to the 4.9 GHz public safety band. You can change the channel width to be able to install more systems in the same area. The available values are 5 MHz, 10 MHz, and 20 MHz (default). The list of available channels vary depending on the chosen bandwidth.
- Bit Rate—The transmission data rate at which the device operates. The Auto value represents the best possible value (with an RF margin of 15 dB) automatically assigned when the connection was established with the other device. It is the default value.

  Once the device is operating properly, Verint strongly recommends to change the configured bit rate from Auto to the actual bit rate of the connection. This way, the wireless communication will be more stable in the presence of changing atmospheric conditions or other RF interferers. To know the actual bit rate of the connection, look in the Advanced > Communication Status and Statistics > Wireless Status menu of the CLI. If the quality of the RF link degrades severely, the actual bit rate could be lower than the manually configured one.

  The available bit rates vary depending on the frequency band:

Band	Channel Bandwidth	Bit Rates (Mbps)
2.4 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54
4.9 GHz	5 MHz	1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5
	10 MHz	3, 4.5, 6, 9, 12, 18, 24, and 27
	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54
5 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54

- Starting Order—A sequence number, used during the boot-up process of a master, to delay its startup. This value is used in a DFS context when frequency channel selection is automatic (see the Channel parameter). The receiver device waits a specific number of seconds based on the value of this parameter. This wait period will ensure that no two receivers will start at the same time and select the same frequency channel. The starting order delay is: (*order* - 1) multiplied by 80 seconds.

The default starting order is 1; every colocated system should have a different value for this parameter if frequency channel selection is automatic.

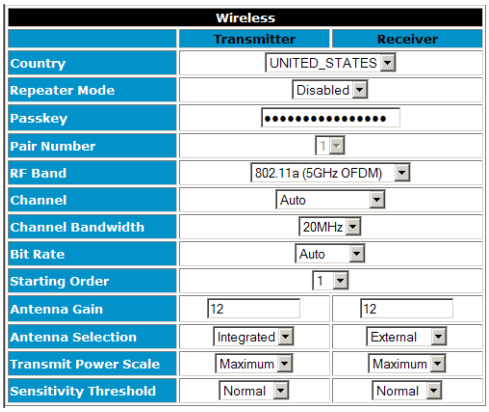
- Antenna Gain—The gain of the antenna on the device (in dBi). You need to enter the gain if you use an external antenna with your device; this way, the device will be able to automatically change its transmission power so that the total power (device and antenna) does not exceed the maximum value established by your country's regulations. If you use the integrated antenna, you should also validate that the proper value for the selected RF band is displayed; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.

NOTE: Providing a gain lower than the actual gain of the antenna you are using is prohibited.

- Antenna Selection—The type of antenna on the device: External if you installed a high-gain antenna on the device; Integrated otherwise.
- Transmit Power Scale—The level of emitting power of the device radio. The default level is the maximum allowed in your country for the configured antenna. If your system operates with a comfortable RF margin (15 dB), you may reduce the emitting power to lower the noise generated on the other RF systems located nearby. The available values are:
  - Maximum
  - 50%—The power is reduced by 3 dB.
  - 25%—The power is reduced by 6 dB.
  - 12.5%—The power is reduced by 9 dB.
- Sensitivity Threshold—The minimum signal level perceived by the radio of the device. Reducing the sensitivity of the radio enables unwanted "noise" to be filtered out. A safe value is 10 dB below the current received signal level; this signal level is displayed in the Wireless connection status (-83 dBm in the illustration on *page 51*). The default value, **Normal**, represents the most sensitive context. You must be careful not to reduce the sensitivity to a level where the device would not "hear" its legitimate correspondent. The available values are Normal, -80 dBm, -75 dBm, -70 dBm, and -60 dBm.

To change the wireless parameters of the devices:

1. In the Unit Wireless Configuration window, click **Advanced Setup**.
2. Locate the **Wireless** area.



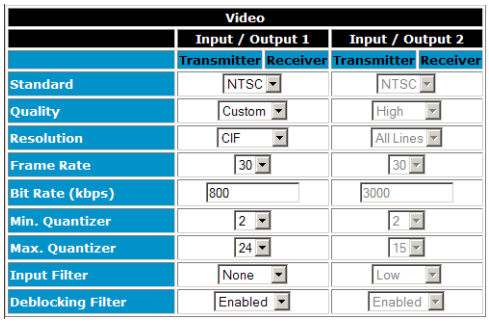
3. Change the desired values.
4. If you are finished with the changes, scroll down the window, then click **Save**. The devices reboot.

The video parameters are the same for both devices in the system. On a -2V system, you have access to a second set of parameters, for the second video input/output. The parameters are:

- Standard—The video standard: either NTSC or PAL.
- Quality—A predefined set of video settings. Each quality represents a predefined set of video settings. Five presets are available: Very Low, Low, Medium, High, and Very High; for their definition, see. If you select a video quality preset, the next parameters in the Video section are unavailable. To change these parameters manually, you have to select the Custom quality.
- Resolution—The measure of how clear and crisp the video image appears. Each resolution corresponds to a specific number of pixels (columns * lines) for each picture of the video sequence.
- Frame Rate—The maximum number of frames per seconds (fps) that will be encoded and transferred by the transmitter. This parameter can be set to 1 to 7, 10, 15, or 30 fps in NTSC mode and 1 to 6, 8, 12, or 25 fps in PAL mode.
- Bit Rate (kbps)—The maximum number of bits per second generated by the device. Valid bit rates range from 9 to 6000 kbps.
- Min. Quantizer—The high video quality boundary. The lower the value, the higher the video quality and the file size. The available values are in the 2–31 range.
- Max. Quantizer—The low video quality boundary. A higher quantizer value means less video quality but a smaller file size. The available values are in the 2–31 range.
- Input Filter—The level of filtering applied to the video signal before it is encoded, helping to remove high frequency noise from lower quality cameras or noisy video feeds. The available values are: None, Low, Medium, and High.
- Deblocking Filter—The indication of whether the deblocking filter is activated. This filter attempts to reduce the blocky artefacts present at the edge of blocks (8x8 pixels).

▶ To change the video parameters of the devices:

1. In the Unit Wireless Configuration window, click **Advanced Setup**.
2. Scroll down to locate the **Video** area.



Video				
	Input / Output 1		Input / Output 2	
	Transmitter	Receiver	Transmitter	Receiver
Standard	NTSC		NTSC	
Quality	Custom		High	
Resolution	CIF		All Lines	
Frame Rate	30		30	
Bit Rate (kbps)	800		3000	
Min. Quantizer	2		2	
Max. Quantizer	24		15	
Input Filter	None		Low	
Deblocking Filter	Enabled		Enabled	

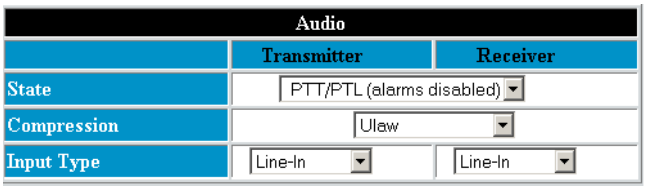
3. Change the desired values. On a *-2V* model, the second column is available for the second video input/output.
4. If you are finished with the changes, scroll down the window, then click **Save**. The devices reboot.

The audio parameters are:

- State—The purpose of Alarm Input 1:
  - Full Duplex (alarms enabled)—Data is transferred in both directions simultaneously. The Alarm Input 1 wire is available for alarms.
  - PTT/PTL (alarms disabled)—A half-duplex mode that allows you to control audio communication between two devices by using a button to switch from voice reception to transmission mode.
  - Audio Disabled (alarms enabled)—There is no audio transfer. The Alarm Input 1 wire is available for alarms.
- Compression—The transfer mode for audio data. The available values are:
  - No Compression—The PCM mode
  - ULaw
  - GSM 6.10
- Input Type—The type of the audio source. The only value is Line-In.

▶ To change the audio parameters of the devices:

1. In the Unit Wireless Configuration window, click **Advanced Setup**.
2. Scroll down to locate the **Audio** area.



Audio		
	Transmitter	Receiver
State	PTT/PTL (alarms disabled)	
Compression	Ulaw	
Input Type	Line-In	Line-In

3. Change the desired values.
4. If you are finished with the changes, scroll down the window, then click **Save**. The devices reboot.

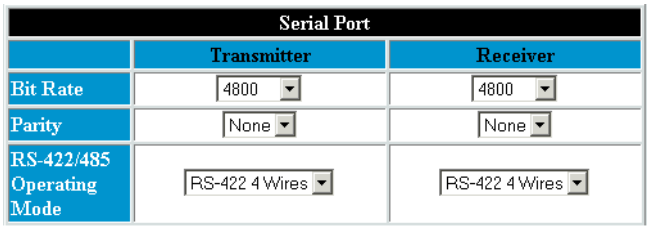
The serial port parameters allowing communication with the target equipment (camera, monitor, and so on) are:

- Bit Rate—The data rate that the serial equipment operates at, in bits per second.

- Parity—The type of parity check. The available values are Odd, Even, or None.
- RS-422/485 Operating Mode—The way the RS-422/485 serial equipment will interface with the device. The available values are: RS-422 4 Wires, RS-485 2 Wires, and RS-485 4 Wires.

▶ To change the serial port parameters of the devices:

1. In the Unit Wireless Configuration window, click **Advanced Setup**.
2. Scroll down to locate the **Serial Port** area.



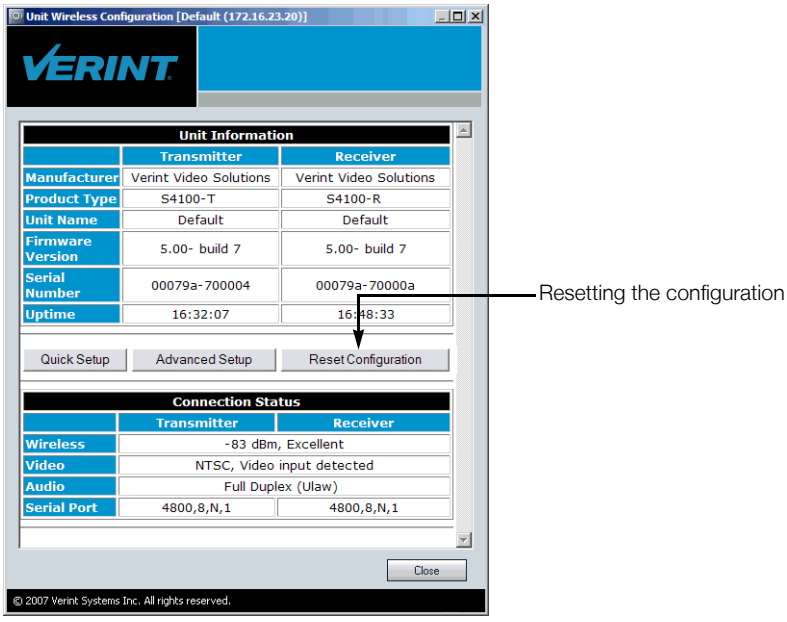
3. Change the desired values.
4. If you are finished with the changes, click **Save**. The devices reboot.

Resetting the Configuration

If the wireless system does not react the way it should, you can load the default configuration in both devices and reboot them. This operation will assign the factory default parameters to each device. All user-defined values will be lost.

▶ To reset the configuration of the S4100 pair:

1. In the Unit Wireless Configuration window, click **Reset Configuration**.



2. In the confirmation window that appears, click **OK**. Both devices receive their default configuration, then they reboot.

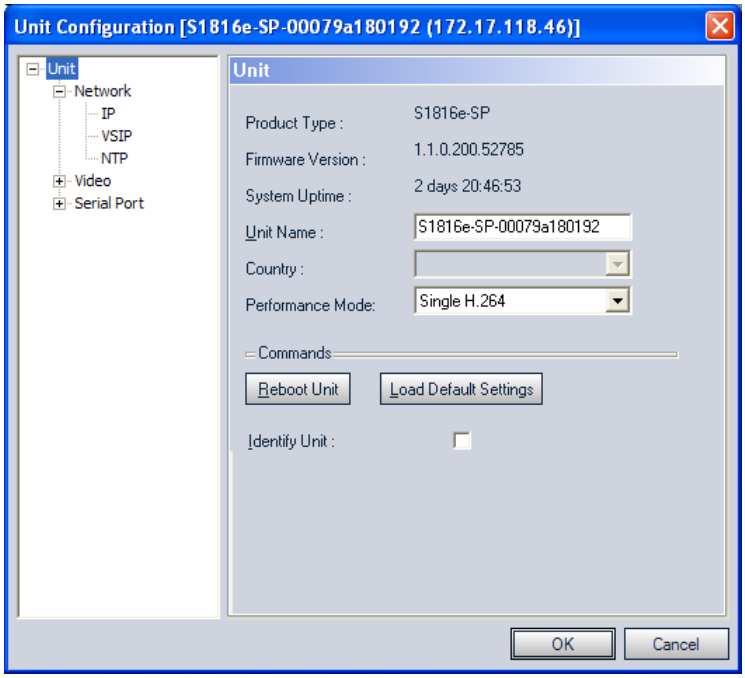
Configuring the S1816e-SP Encoder

The S1816e-SP is a cost effective encoder with performance of up to 4CIF/15 frames per second. The S1816e-SP supports H.264 and MPEG-4 video on all 16 ports and can be configured in dual or triple stream modes. By default, the S1816e-SP is configured in single H.264 mode.

Use SConfigurator to select the mode of the unit. Once you have set the mode, it will take effect once you have rebooted the unit.

▶ To change the performance mode for the S1816e-SP:

1. Double-click `SConfigurator.exe` to start SConfigurator.
2. Select the **Units** tab, then click **Discover**.
3. Select the S1816e-SP encoder and click **Configure**.



4. In the **Unit Name** box, from the Performance Mode list, select the streaming mode for H.264. You can select from:
   - Single H.264: One H.264 stream and one MPEG-4 stream per video input.
   - Dual H.264: Two H.264 streams with lower resolution and frame rate and one MPEG-4 stream per video input..
5. Click **Reboot Unit** for the change to take effect.
6. Click **OK** to close the Unit Configuration dialog box.
7. Click **Exit** to close SConfigurator.

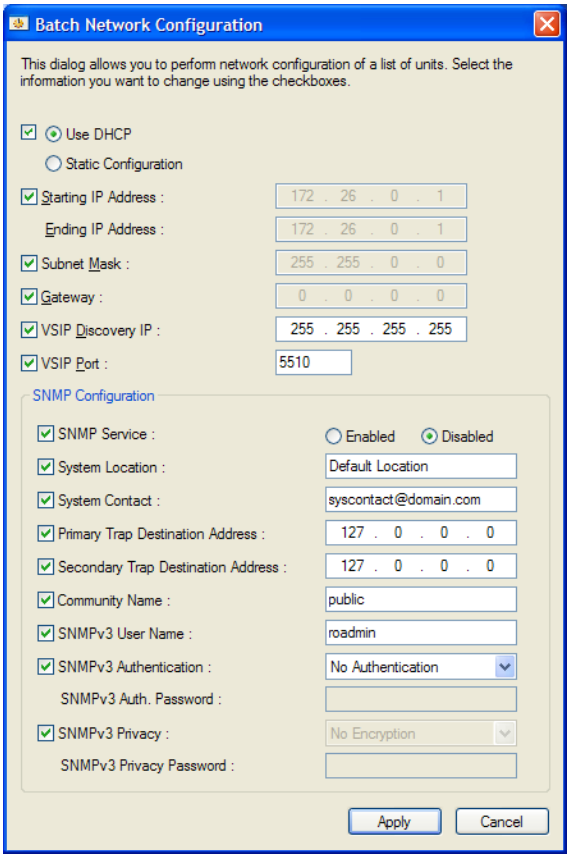
CAUTION: Once you have added the S1816e-SP encoder to Nextiva VMS, changing the mode requires that you delete the encoder from Nextiva VMS and use SConfigurator to change the mode. then re-add the S1816e-SP encoder back to Nextiva VMS.

Performing a Batch Network Configuration

You can configure the IP network and SNMP parameters of a batch of devices belonging to the same subnet in a single operation. Two methods are available to set the IP addresses: DHCP or manual. For more details on DHCP, see *Appendix A: DHCP Support and APIPA*.

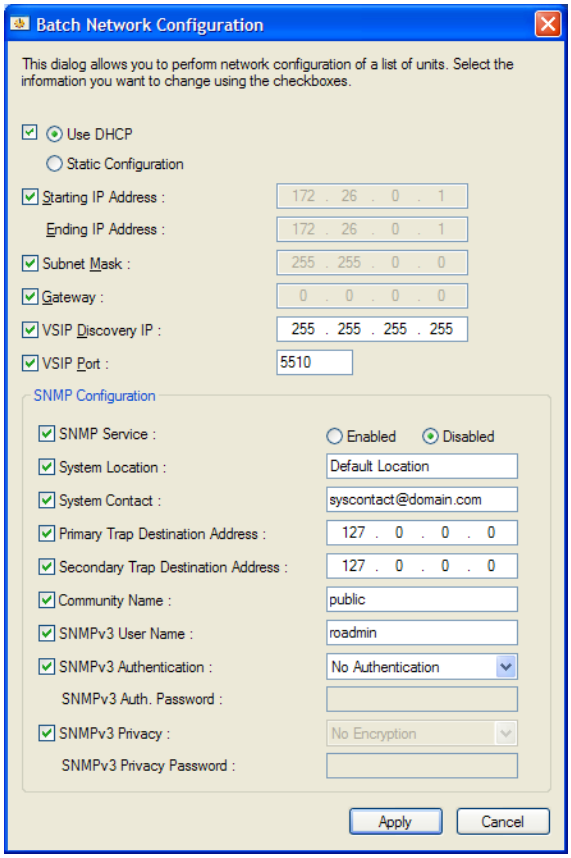
▶ To perform a batch network configuration:

1. In the Units box, hold down either the **Ctrl** (non-contiguous selection) or **Shift** (contiguous selection) key while selecting the devices to be configured.
2. Right-click in the selection, then select **Batch Network Configuration** from the contextual menu. The Batch Network Configuration window appears.


Batch Network Configuration
This dialog allows you to perform network configuration of a list of units. Select the information you want to change using the checkboxes.
Use DHCP
Static Configuration
Starting IP Address : 172 . 26 . 0 . 1
Ending IP Address : 172 . 26 . 0 . 1
Subnet Mask : 255 . 255 . 0 . 0
Gateway : 0 . 0 . 0 . 0
VSIP Discovery IP : 255 . 255 . 255 . 255
VSIP Port : 5510
SNMP Configuration
SNMP Service : Enabled Disabled
System Location : Default Location
System Contact : syscontact@domain.com
Primary Trap Destination Address : 127 . 0 . 0 . 0
Secondary Trap Destination Address : 127 . 0 . 0 . 0
Community Name : public
SNMPv3 User Name : roadmin
SNMPv3 Authentication : No Authentication
SNMPv3 Auth. Password :
SNMPv3 Privacy : No Encryption
SNMPv3 Privacy Password :
Apply
Cancel

3. To assign IP addresses with a DHCP server, check **Use DHCP**. The next four boxes become greyed out.
4. Enter the network information as required. In manual mode, you do not have to enter the ending IP address since it is automatically assigned according to the number of devices to configure: The address of each device is incremented by one.

5. To change a subset of the parameters, click **Select Subset**, then select the desired parameters by checking or clearing boxes to their left. For example:

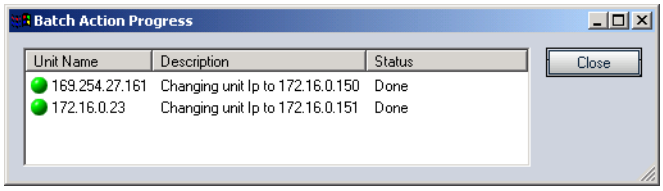

Batch Network Configuration
This dialog allows you to perform network configuration of a list of units. Select the information you want to change using the checkboxes.
Use DHCP
Static Configuration
Starting IP Address : 172 . 26 . 0 . 1
Ending IP Address : 172 . 26 . 0 . 1
Subnet Mask : 255 . 255 . 0 . 0
Gateway : 0 . 0 . 0 . 0
VSIP Discovery IP : 255 . 255 . 255 . 255
VSIP Port : 5510
SNMP Configuration
SNMP Service : Enabled Disabled
System Location : Default Location
System Contact : syscontact@domain.com
Primary Trap Destination Address : 127 . 0 . 0 . 0
Secondary Trap Destination Address : 127 . 0 . 0 . 0
Community Name : public
SNMPv3 User Name : roadmin
SNMPv3 Authentication : No Authentication
SNMPv3 Auth. Password :
SNMPv3 Privacy : No Encryption
SNMPv3 Privacy Password :
Apply
Cancel

NOTE: Do not clear the check box to the left of **Use DHCP**, because it sends to the devices the indication of whether or not to use a DHCP server for the batch configuration. Typically, when selecting only a subset, you do not use DHCP, so leave the check box to the right of Use DHCP cleared.

6. In the **SNMP** panel, select the **Enabled** check box enable the SNMP service.
7. In the **System Location** box, type the location for the Edge device.
8. In the **System Contact** box, type the e-mail address of the network administrator.
9. In the **Primary Trap Destination Address** box, type the IP address of the primary server that will receive the SNMP Traps.
10. In the **Backup Trap Destination Address** box, type the IP address of the backup server that will receive the SNMP Traps in case the primary server is unavailable.
11. In the **Community Name** box, type the name of the group where you want the edge device to be a member.

NOTE: The Edge device will only respond to requests from management servers that belong to the same community.

12. In the **SNMPv3 User Name** box, type the name of the SNMP user.
13. In the **SNMPv3 Authentication** list, select the authentication algorithm for SNMP requests. You can select from the following.
    - No Authentication: No authentication is used.
    - MD5 Authentication: The Message Digest Version 5 (MD5) hash function is used to determine that the message is from a valid source.
    - SHA Authentication: The Secure Hash Algorithm (SHA) has function is used to determine that the message is from a valid source.
14. In the **SNMPv3 User Auth Password** box, type a password for the user.
15. In the **SNMPv3 Privacy Protocol** list, select the privacy protocol to encrypt the contents of the data. You can select from the following:
    - No Encryption: No encryption is used.
    - DES Encryption: The Data Encryption Standard (DES) algorithm is used to encrypt the data.
    - AES Encryption: The Advanced Encryption Standard (AES) algorithm is used to encrypt the data.
16. In the **SNMPv3 Privacy Password** box, type a password for the privacy protocol.
17. To start the batch process, click **Apply**. The Batch Action Progress window appears, showing the status of each device.



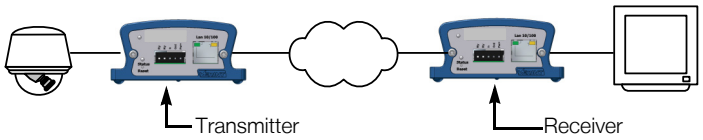
18. When all devices have been configured, click **Close**. The devices will reboot with their new configuration.

Chapter 3

Managing Connections

Adding a Connection. 63
Removing a Connection 65

A point-to-point connection is the association of a transmitter (or an IP camera) and a receiver to view video coming from an analog camera on an analog monitor.



SConfigurator can manage point-to-point connections on the IP network. It allows you to add or remove connections between a transmitter and a receiver.

Adding a Connection

To create a point-to-point connection between a transmitter and a receiver, both must be part of the Units box (in the Units tab).

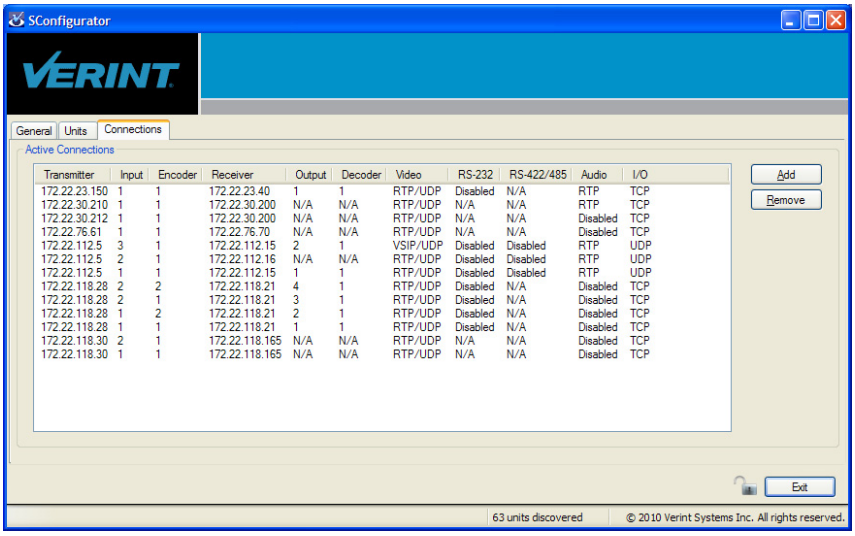
NOTE: The S1700e and S1800e multiport series transmitters does not support point-to-point connections.

The available receivers are the S1970e-R and the S1504e-R. You can connect each of these receivers to up to four transmitters, to create a maximum of four different point-to-point connections.

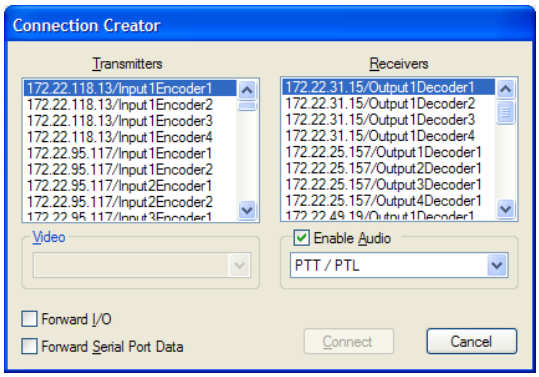
In addition to video, you can use a point-to-point connection to transfer audio, input/output (for example, alarms and events), and serial port (like PTZ commands); however, if one of the two devices does not have one of these features, you will not be able to include it in the connection.

▶ To create a connection:

1. In S1900e-Vicon, click the **Connections** tab. The existing connections are displayed.


SConfigurator
VERINT
General
Units
Connections
Active Connections
Transmitter Input Encoder Receiver Output Decoder Video RS-232 RS-422/485 Audio I/O
172.22.23.150 1 1 172.22.23.40 1 1 RTP/UDP Disabled N/A RTP TCP
172.22.30.210 1 1 172.22.30.200 N/A N/A RTP/UDP N/A N/A RTP TCP
172.22.30.212 1 1 172.22.30.200 N/A N/A RTP/UDP N/A N/A Disabled TCP
172.22.76.61 1 1 172.22.76.70 N/A N/A RTP/UDP N/A N/A Disabled TCP
172.22.112.5 3 1 172.22.112.15 2 1 VSIP/UDP Disabled Disabled RTP UDP
172.22.112.5 2 1 172.22.112.16 N/A N/A RTP/UDP Disabled Disabled RTP UDP
172.22.112.5 1 1 172.22.112.15 1 1 RTP/UDP Disabled Disabled RTP UDP
172.22.118.28 2 2 172.22.118.21 4 1 RTP/UDP Disabled N/A Disabled TCP
172.22.118.28 2 1 172.22.118.21 3 1 RTP/UDP Disabled N/A Disabled TCP
172.22.118.28 1 2 172.22.118.21 2 1 RTP/UDP Disabled N/A Disabled TCP
172.22.118.28 1 1 172.22.118.21 1 1 RTP/UDP Disabled N/A Disabled TCP
172.22.118.30 2 1 172.22.118.165 N/A N/A RTP/UDP N/A N/A Disabled TCP
172.22.118.30 1 1 172.22.118.165 N/A N/A RTP/UDP N/A N/A Disabled TCP
Add
Remove
Exit
63 units discovered
© 2010 Verint Systems Inc. All rights reserved.

2. Click **Add**. The Connection Creator window appears.



3. Select a transmitter in the left column and a receiver in the right one. In the Transmitters column, you have access to all the encoders of each input. The video stream is the same for both. Encoder1 is always reserved for viewing live video with the web interface, therefore you should use Encoder2 for point-to-point connections; however, you can use the same encoder for both functions if you want the same resolution and frame rate.
4. In the **Video** list, select the desired transmission mode for video data. Depending on the edge device and the firmware version, the following modes may be available:
   - **RTP/UDP**—A video mode using RTP (Real Time Transport Protocol, RFC 3550) over the UDP protocol. It is the preferred mode for LAN environments; however, it does not guarantee proper reception of packets. (default)
   - **VSIP/UDP**—A legacy mode, using the proprietary VSIP video protocol over UDP. The preferred UDP mode is RTP/UDP.
   - **RTP/TCP**—A video mode using RTP (Real Time Transport Protocol, RFC 3550) over the TCP protocol. It can be useful over WANs, Internet, or LANs needing more robust or secure connections. This mode guarantees proper reception of packets, but could slow down the effective frame rate to a level which is not acceptable.
   - **VSIP/TCP**—A legacy mode, using the proprietary VSIP video protocol over the TCP protocol. The preferred TCP mode is RTP/TCP.
5. If you are not transferring I/O data (typically alarms) between the two selected devices, clear **Forward I/O**.
6. If you are not transferring serial port data (like PTZ commands), clear **Forward Serial Port Data**.
7. To enable audio between the devices, ensure that **Enable Audio** is checked, then select the mode. The available audio modes are:
   - **Full Duplex**—Audio data is transferred in both directions simultaneously.
   - **PTT/PTL**—The push-to-talk/push-to-listen mode allows you to control audio communication by using a button to switch from voice reception to transmission mode. Audio data will be transmitted only if the PTT or PTL buttons are pressed.

NOTE: On the S1970e-R, you can activate audio on a single connection only. The active audio connection is the last that was performed.
The audio connection will remain the same even if the S1970e-R is in guard tour mode, that is, the receiver will not switch between the audio streams of its four connected transmitters.

8. Click **Connect**.

You should now have video on the monitor connected to the receiver device. Audio, I/O, and serial port can also be transferred.

Removing a Connection

You can remove an existing point-to-point connection between two devices. Removing a connection means that no more data will be transmitted between the two.

▶ To remove a connection:

1. In the Active Connections box of the Connections tab, select a connection, then click **Remove**. A confirmation window appears.
2. Click **OK**.

Chapter 4

Enabling Security

Building a Secure System 67
Adding a Device to the Trusted List 68

You can enable the SSL (Secure Sockets Layer) protocol in SConfigurator and in the SSL-enabled edge devices. Therefore, the connections between SConfigurator and a device or between two devices can be secure.

Building a Secure System

SSL is a commonly used protocol for managing the security of message transmission on an IP network. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate; therefore, each SSL-enabled device comes with its own unique SSL certificate.

The SSL protocol secures the following data: I/O, serial port, and VSIP communication. It does not apply to audio and video transmission.

For increased security, assign a common SSL passkey to the SmartSight devices and SConfigurator. To establish a secure system, it is strongly recommended to change the default passkey (the empty string) prior to putting the devices in production.

Another security measure is the list of devices that SConfigurator trusts. If you use that list, fake devices with SSL certificates or hacked SConfigurator programs will not be able to break into your secure system.

▶ To build a secure system:

1. Create the list of devices that will work in the secure context (see *page 6*). This list is called the *trusted list*, and the enclosed devices, the *trusted devices*.
2. Set up the default secure VSIP connection between SConfigurator and a new device:
   a. In the Program Options window, set the SConfigurator VSIP port to 5510 and the SSL passkey to the empty string (see *page 4*).
   b. On the edge device, set the VSIP port to 5510 (see *page 19*) and the SSL passkey to the empty string (see *page 21*).

      If the device is new, it already has these factory default parameters.
   c. Discover the device (see *page 7*).
3. For a wired transmitter, wired receiver, IP camera, or S4200 series wireless transmitter, change its SSL passkey (see *page 21*) and VSIP port (see *page 19*).
4. For an S1100w wireless transmitter, change its wireless passkey (see *page 29*).
5. For an S3100 series or S4300 series device:
   a. Change its SSL passkey (see *page 21*) and VSIP port (see *page 19*).
   b. Change its wireless passkey (see *page 29*).
6. Add the device to the trusted list (see *page 68*).
7. Enable security in the device (see *page 21*).
8. Repeat steps *Step 2* to *Step 7* for each device to be part of the secure system, with the same SSL passkey and VSIP port.

9. Secure SConfigurator:
   a. Change its VSIP port to the value assigned to the devices (see *page 4*).
   b. Assign it the same SSL passkey as the devices, then enable its security (see *page 6*).

Adding a Device to the Trusted List

You can add a configured device to the list of devices that SConfigurator SSL-trusts. If the trusted device list is not yet created, see *page 6*.

▶ To add the device to the trusted list:

1. In the Units box, right-click the device.
2. From the contextual menu, select **Security > Trust Unit**.

The device is added to the trusted list. In the Units box, its value in the Trusted column turns to **Yes**.

Chapter 5

Updating Firmware

Performing the Update 70
Firmware Update Messages 71

You can use SConfigurator to update the firmware of SmartSight edge devices.

NOTE: Firmware downgrade is not supported on any device. If you perform a downgrade, any problem encountered will not be covered by your product warranty.

Performing the Update

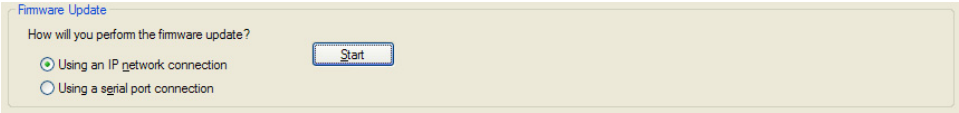
You may need to update an edge device to have access to improved firmware or new features. Updating the firmware of a device retains its configuration.

The latest firmware files are available on the Verint Video Intelligence Solutions extranet (Quick Links > Firmware and Applications > SmartSight Intelligent Edge Devices).

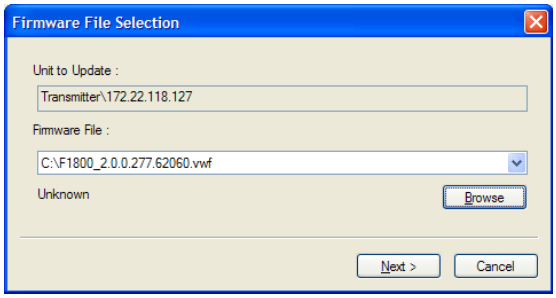
The preferred method to update the firmware of all devices is through an IP network connection. On the S1100w and the S1504e-R, you can also perform it with a serial port.

▶ To update the firmware using an IP network connection:

1. In the Units tab, select the device to update.
2. In the **Firmware Update** box, select **Using an IP network connection**.


Firmware Update
How will you perform the firmware update?
Using an IP network connection
Using a serial port connection
Start

3.
4. Click **Start**. The Firmware File Selection window appears.



5. Click **Browse**, select the desired firmware file, then click **Open**.
6. Click **Next**. The Firmware Update window appears.
7. Click **Start**. The Firmware Update Progress window appears.

   The update procedure may take several minutes to complete. For a list of status messages, see *Firmware Update Messages* on *page 71*.

If the update procedure fails:

1. Restart the same procedure immediately.
2. If the problem persists, reboot the device, then restart the update procedure.
3. If the problem persists, look at the status LED for abnormal behavior.

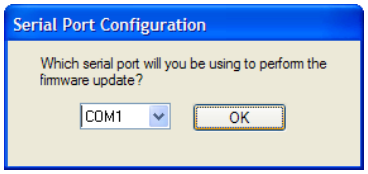
You should take into consideration the following facts regarding firmware updates using the IP network:

- It can be deactivated in the command line interface (CLI).
- Ensure that the IP link is stable before starting the procedure; therefore it is not recommended to perform it over the Internet.

▶ To perform the firmware update using a serial port connection:

NOTE: SConfigurator needs a COM port to perform firmware update. You need to disable any program using this port prior to starting this procedure.

1. Connect the host computer to the SmartSight device via the RS-232 serial port.
2. In the Units tab, select the device to update.
3. In the **Firmware Update** box, select **Using a serial port connection**.
4. Click **Start**. The Serial Port Configuration window appears.



5. Select the serial port to use, then click **OK**. The Firmware File Selection window appears.
6. To open the desired firmware file, click **Browse**, then select it.
7. Click **Next**. The Perform Update window appears.
8. Click **Start**. The Firmware Update Progress window appears, displaying a progress bar and status messages. The update procedure may take several minutes to complete.

Firmware Update Messages

During firmware updates, many messages appear in the Firmware Update Progress window. The most frequent include:

Another program is using the selected com port. Try again after the other program completes.
: SConfigurator cannot open the communication port. Check that you are using the correct COM port or if it is being used by another application.

Can't establish a connection to remote device via IP.
: SConfigurator cannot establish a connection with the device. The device may be powered down or disconnected from the network.

Can't receive data via the serial port.
: If this message appears before the update process, ensure that you have properly quit the CLI (by pressing q in the main menu). If this message appears during the process, you will need to reboot the device because it is in backup mode. Try performing another update using the serial port or IP connection. If the problem persists, contact customer service.

Communication established.
: SConfigurator is now communicating with the device.

Error: Invalid firmware file.

Select a valid file or ensure that the file exists. If the problem persists, contact customer service to get a valid file.

Firmware upload done.

The update process has been completed successfully.

Firmware upload request sent.

SConfigurator has made a request to the SmartSight device for update.

Invalid mih/smih file.

Select a valid file or ensure that the file exists. If the problem persists, contact customer service to get a valid file.

The firmware update failed.

A problem occurred during firmware update. The update process has not been completed successfully.

Chapter 6

Aligning the Antenna

Aligning the External Antenna 74

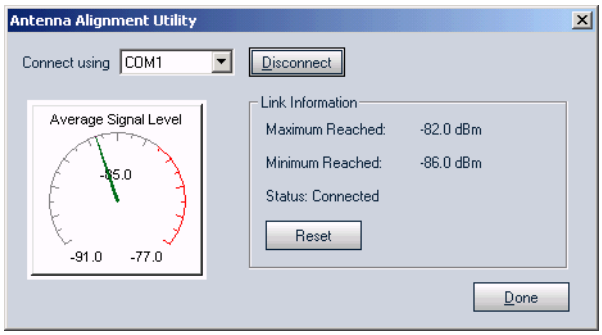
Aligning the External Antenna

SConfigurator supplies a graphical environment to help you align the external antenna of an S1100w, S4200 series, slave S3100 series, or slave S4300 series with that of its connected master.

NOTE: The antenna alignment utility works only with devices whose firmware release is 2.55 or higher.

▶ To align the external antenna:

1. In the General tab, click **Antenna Alignment**. The Antenna Alignment Utility window appears.



   - On an S1100w device:
     - Connect the device to a COM port of the host computer using a serial cable.
     - In the **Connect using** box, select the COM port, then click **Connect**.
   - On a S4200 series, slave S3100 series, or slave S4300 series:
     - In the **Connect using** box, select **Telnet**, then click **Connect**.

       The Telnet Connection window appears.
     - Enter the IP address of the slave device, then click **OK**.

       Wait until the status becomes **Connected**.
2. Move the antenna so as to get the highest signal level possible (that is, the closest to 0 dBm). The needle in the Average Signal Level dial moves to indicate the current radio signal (in dBm). A red arc around the dial indicates the best values reached so far. The dial automatically adjusts its range in real time to improve reading precision.
3. To recalibrate the dial and reset the minimum and maximum values reached, click **Reset**.
4. Click **Done** to exit.

Chapter 7

Managing the Licenses

Creating a License Request File 76
Installing Licenses 77
Assigning a Package 79
Removing a License 81

Verint introduces a licensing scheme to allow customers to access specialized features that they bought for their Verint edge devices. Currently, only the analytics feature is licensable (to be more precise, the content analyzer VSIP capability); however, the licensing scheme is generic enough to support other features. For more information about the licensing scheme or the analytics feature, refer to the Verint *Edge Device Analytics SDK Programmer Guide*.

NOTE: Licenses are not included in firmware files. You need to purchase them separately.

The analytics-ready edge devices are the S1704e-AS, S1708e-AS, S1900e-AS, S2600e-AS, and S2610e-AS.

S1900e-Vicon allows you to perform the following operations relative to licensing:

- Creating a license request file
- Installing a license on an edge device
- Assigning a package to an input
- Removing a license

Creating a License Request File

The easiest way to order a license from Verint Customer Service is to create a license request file. You can create such a file for many devices at the same time, provided they are of the same product type (for example, three S1900e-AS devices) and they require the same packages.

When you request a license, you provide the number of required packages for the edge device. For the content analyzer licensable capability, three package types are available:

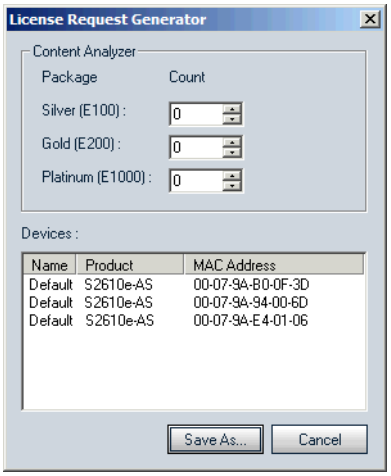
- Silver (E100)
- Gold (E200)
- Platinum (E1000)

The package types represent the sensors that can be assigned on the video inputs of the device. For multiport devices, you can order as many packages as there are video inputs.

▶ To generate a license request file:

1. In the Units tab, select the devices for which a license is required. To select multiple devices of the same type, hold down either the **Ctrl** (non-contiguous selection) or **Shift** (contiguous selection) key.

2. Right-click in the selection, then select **Licensing > Generate License Request File**. The License Request Generator window appears.



3. In the Content Analyzer group box, select the desired number of packages for the device. If you are requesting licenses for many devices of the same type, provide values for a single device; for instance, enter a single **1** for the three S2610e-AS devices in the illustration since each device can receive a single package. For multiport devices, you may select different package types. You must order at least one package.
4. Click **Save As**.
5. Specify a location and a name for the license request file, then click **Save**. The license request file is generated.
6. Send the license request file to Verint Customer Service.

Installing Licenses

You can install many licenses on several devices in a single operation, or perform this operation one device at a time.

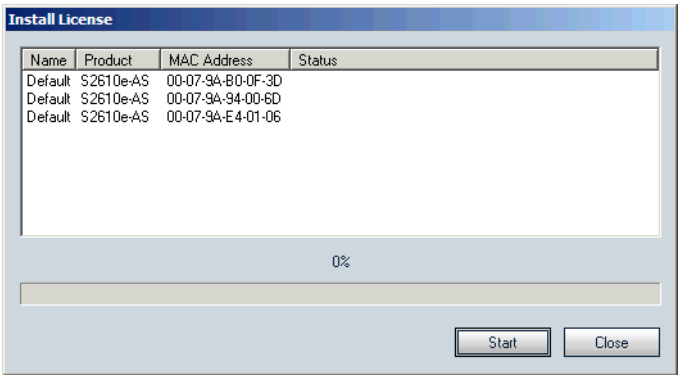
To install many licenses in batch mode, you need a single aggregated file containing all the desired licenses. This file was generated by Verint Customer Service. S1900e-Vicon will use only the required licenses by comparing the MAC addresses of the edge devices with the contents of the aggregated file; remaining licenses may be installed later.

Only one license can be present in a device at any time; therefore, you must remove it before an upgrade or to move it to another edge device.

▶ To perform a batch license installation:

1. In the Units tab, perform one of the following operations:
   - To install licenses on all discovered devices, right-click any device, then select **Licensing > Install License on All Units**.
   - Select the devices for which a license is required, right-click in the selection, then select **Licensing > Install License on Selected**.

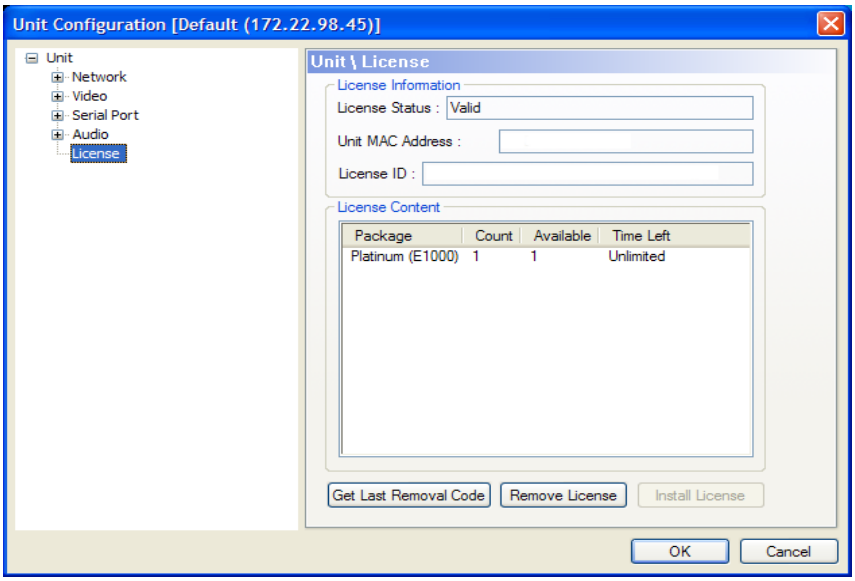
2. In the Open window, select the aggregated file, then click **Open**. The Install License window appears.



3. Click **Start**. The licenses are installed one after the other. If the operation is successful, the status of the device becomes **OK: Success** and the device reboots. If an error occurs, the status displays a descriptive message.
4. When all licenses are installed, click **Close**. The contents of the Units tab is refreshed. The license status of the devices becomes **Valid**.

▶ To install a single license:

1. In the Units tab, double-click the desired device.
2. In the parameter tree, click **License**.



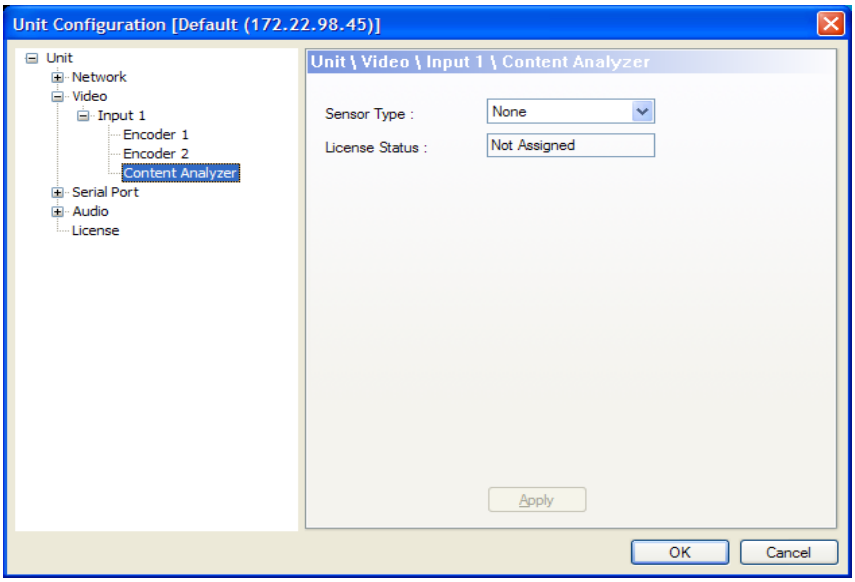
3. Click **Install License**.
4. In the Open window, select the license request file, then click **Open**. The license is installed.
5. In the message window indicating that the device is rebooting, click **OK**. The contents of the Units tab is refreshed. The license status of the device becomes **Valid**.

Assigning a Package

After installing a license in a device, the next step is to assign packages to the video inputs.

▶ To assign a package to a video input:

1. In the Units tab, double-click the desired device.
2. In the parameter tree, expand the **Video** and the desired **Input** nodes, then click **Content Analyzer**.

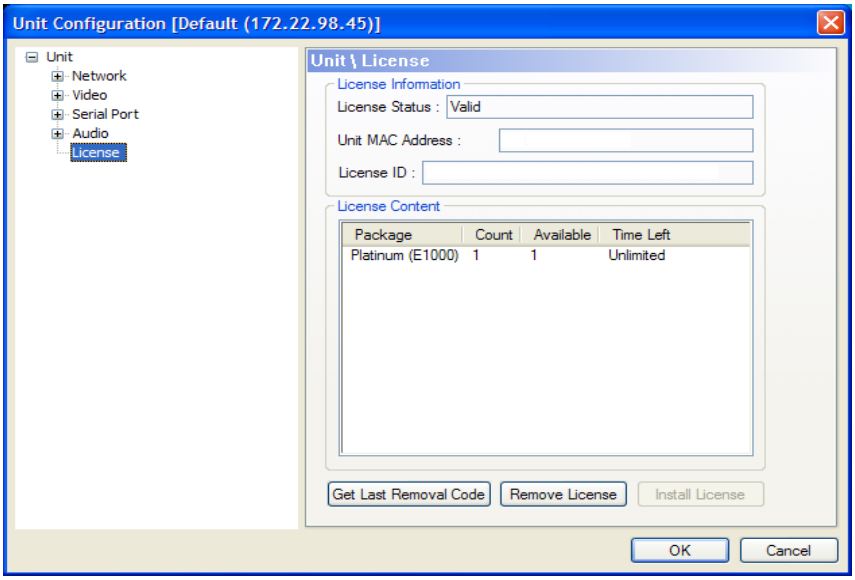


3. In the **Sensor Type** list, select the package to assign to the content analyzer, then click **Apply**. Only unassigned packages will be part of the Sensor Type list. The License Status is updated and should read Valid.

▶ To view the package assignment of a license:

1. In the Units tab, double-click the desired device.

2. In the parameter tree, click **License**. The License Information group box is filled with data coming from the license file.



The License Content group box contains the information relative to the packages:

- Package—A package type that is available in the device.
- Count—The total number of packages of that type in the license.
- Available—The number of packages of that type that are available for assignment.
- Time Left—For a trial license, the remaining time. The other available values are **Expired** (when the trial period is over) or **Unlimited** (for a non-trial package).

Removing a License

You need to remove a license from an edge device if you need to upgrade it or move it to another edge device. You cannot re-use a removed license.

To move a license to another device, you need to send a removal code to Verint Customer Service. You can retrieve the removal code at any time until another license is uninstalled on the same device.

▶ To remove a license:

1. In the Units tab, double-click the desired device.
2. In the parameter tree, click **License**.

   The License Status box should indicate Valid.
3. Click **Remove License**.

   The license is removed.
4. In the message window indicating that the device is rebooting, click **OK**.

   The contents of the Units tab is refreshed. The license status of the device becomes Not Installed.

▶ To get a removal code:

1. In the Units tab, double-click the desired device.
2. In the parameter tree, click **License**.
3. Click **Get Last Removal Code**. The Last Removal Code window appears.
4. Click **Save As**, enter a location and file name for the code, then click **Save**.
5. Send the file to Verint Customer Service.

Chapter 8

Troubleshooting an Edge Device

Troubleshooting 83

This chapter contains frequently asked questions relative to security and device discovery using SConfigurator.

Troubleshooting

What exactly is a secure VSIP connection? Is it the same as an SSL connection?

A secure VSIP connection is a connection that is secured with SSL between SConfigurator and a device. This type of connection is also called *SSL* or *TCP-secured*.

To have a secure connection, you need the following prerequisites:

- The VSIP connection type must be TCP (the default value). If you change it manually to UDP in the CLI, no secure connection is possible.
- The SSL passkeys in the device and in SConfigurator must be the same.
- Obviously, SConfigurator and the device must have the same VSIP port (otherwise, the device will not be visible in the Units tab).

How come a secure VSIP connection can exist between a device and SConfigurator even if security is not enabled in them?

Enabling security in SConfigurator and in a device only implies that they will not accept insecure connections anymore. As long as they share the same SSL passkey and the same VSIP port, their connection is secured with SSL.

I just enabled security on a device and added it to the trusted list. How come it becomes Unknown in the Units box and its VSIP connection turns to UDP instead of SSL?

The VSIP connection between the device and SConfigurator is not secure because their SSL passkeys do not match. Remember that activating security on a device implies that it does not accept insecure connections anymore. As soon as the passkeys are the same, the VSIP connection will switch to SSL, and SConfigurator will be able to talk to the device and display its information.

How come I can add a device without an SSL certificate in the trusted list?

There is no link between SSL and the trusted list. You can include any device you want in the trusted list. However, if you enable security in SConfigurator, it will not be able to communicate with non-SSL devices anymore: The information on the devices will change to *Unknown* in the Units box.

How come no devices appear in the Units box after I clicked the Discover button, even though I know there are many of them in the same LAN?

The VSIP port is not the same in SConfigurator and in the devices.

How come I do not see the new devices I just connected on my network, after clicking the Discover button?

To be able to view the new devices, you must activate the Detect All Units on LAN parameter in the Program Options (in the General tab). Since the IP addresses of such devices are always 169.254.*X*.*Y*, they are not in the same subnet as the computer running SConfigurator. You should also ensure that the VSIP port is the same in SConfigurator and in the devices.

However, you should not leave this parameter activated after configuring your devices, since it slows down the discovery process on your network.

How come I get an error message—specifying that the device cannot be located—after I entered the correct IP address of a device with the Add button?

The VSIP port is not the same on SConfigurator and the device to be added.

How come I cannot change the SSL passkey of a device in the Network configuration tab, even though I know that it has a digital certificate?

The source of this problem is that the VSIP connection with SConfigurator is not secure. To solve the problem, you need to change the SSL passkey of the device through the CLI. As soon as the passkey is the same in the device and in SConfigurator, the VSIP connection becomes secure; you can then change the passkey in the Network tab.

How come many devices become unknown after I activated security in SConfigurator?

The following devices will become unknown in the Units box:

- Those without an SSL certificate
- Those not part of the trusted list
- Those not sharing the same SSL passkey

Appendix A

DHCP Support and APIPA

Understanding DHCP and APIPA 86

Understanding DHCP and APIPA

DHCP (Dynamic Host Configuration Protocol) allows devices and computers connected to a network to automatically get a valid IP configuration from a dedicated server.

The APIPA (Automatic Private IP Addressing) scheme, available on the Windows operating systems, enables a device to assign itself a temporary IP address.

At startup, an edge device searches for a valid IP network configuration. The device requires this configuration prior to starting its functions. The network configuration for Nextiva devices consists of:

- An IP address
- A subnet mask
- A gateway

By default, the device tries to contact a DHCP server. If DHCP configuration fails—if the device does not find a server or if it cannot get a configuration from it within one minute—the device assigns itself temporary network parameters based on the APIPA addressing scheme. This scheme allows a device to find a unique IP address until it receives a complete network configuration, either manually or from a DHCP server.

A device in APIPA mode does not reside on the same subnet as the other devices on the IP network; therefore, it may not be able to view or be visible by the other devices. Devices use the following temporary APIPA configuration:

- IP address: 169.254.*X.Y* (where *X* and *Y* are based on the last two digits of the MAC address of the device)
- Subnet mask: 255.255.0.0
- Gateway: 169.254. *. *

A device is in APIPA mode:

- After receiving a duplicate IP address
- When the DHCP server does not have any available IP addresses

DHCP configuration is automatically enabled after a factory reset.

Appendix B

Accessing the CLI

Accessing the CLI 88

Accessing the CLI

For edge devices older than the S1800e series, you may need to access the command line interface (CLI) to perform troubleshooting tasks, typically with the assistance of a Verint customer service specialist. The CLI is hierarchically organized, with menus, sub-menus, and individual options representing configuration parameters.

You can access the CLI using the serial port or the Telnet terminal emulation program. On the S1100w, S1504e-R, and multiport S1700e series devices, you can access the CLI through an RS-232 serial port.

For the S1800e series edge devices, Verint provides a new Web Interface that has all the same functionality as the CLI, but with a simple and intuitive design. For more information on the Web Interface, refer to the Web Interface User Guide.

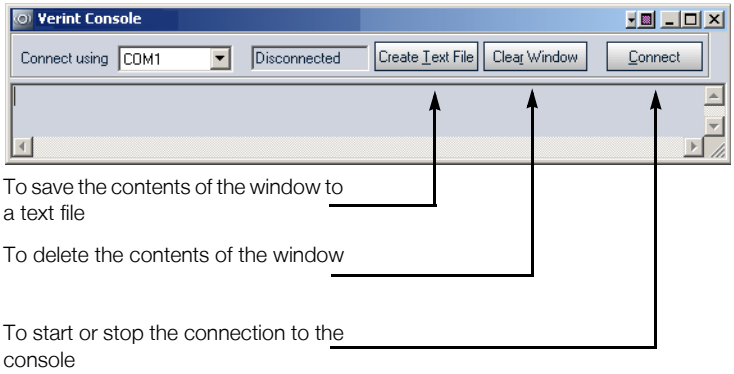
NOTE: Verint recommends that you use the new Web Interface to configure and perform troubleshooting tasks for the S1800e series edge devices.

▶ To access the Web Interface of the S1800e series edge devices:

- In a web browser, type the IP Address of the S1800e edge device.

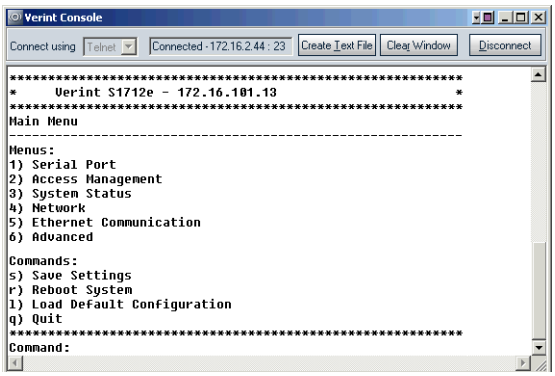
▶ To access the CLI of an edge device:

1. To access the CLI through a serial port:
   a. Connect the device to a COM port of the computer using a serial cable.
   b. In the General tab, click **Console**. The Verint Console window appears.



   c. In the Connect using list, select the COM port used to communicate with the device.

d. Click **Connect**. The CLI main menu appears.



2. To access the CLI with Telnet, select the desired device in the Units tab, then click **Telnet**. The CLI main menu appears.

   The CLI has a timeout that is triggered after three minutes of inactivity. When the timeout occurs:

   - You lose access to the command line.
   - The “Thank you for using the Verint CLI.” message appears at the command line.
   - The Verint Console window becomes disabled.
   - The Disconnect button switches to **Connect**.

3. To reactivate the CLI after a timeout, click **Connect**.
4. To work through the CLI menu structure, follow these guidelines:
   - To execute a command or open a menu, type in the corresponding letter or number, then press **Enter**.
   - To return to the previous menu, enter **p**.
5. To end the CLI work session:
   a. Save the parameters by entering **s** at the main menu, then pressing **Enter**.
   b. Exit the CLI by entering **q** at the main menu, then pressing **Enter**.
   c. Close the Verint Console window.

NOTE: Do not use the Disconnect button to exit the CLI, since it does not save your settings and does not free the RS-232 connection (if applicable).

Glossary

This glossary is common to the Verint line of edge device products.

Access Point

A communication hub for connecting wireless edge devices to a wired LAN.

AES

(Advanced Encryption Standard) An encryption standard used in the WPA2 authentication method.

APIPA

(Automatic Private IP Addressing) A feature of Windows-based operating systems that enables a device to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function. Also known as *AutoIP*.

Bridge

See *Wireless Bridge*.

CCTV

(Closed Circuit Television) A television system in which signals are not publicly distributed; cameras are connected to television monitors in a limited area such as a store, an office building, or on a college campus. CCTV is commonly used in surveillance systems.

CIF

(Common Intermediate Format) A video format that easily supports both NTSC and PAL signals. Many CIF flavors are available, including CIF, QCIF, 2CIF, and 4CIF. Each flavor corresponds to a specific number of lines and columns per video frame.

CLI

(Command Line Interface) A textual user interface in which the user responds to a prompt by typing a command.

Codec

(Coder/Decoder) A software library that compresses or decompresses a video stream following a specific protocol.

Configuration Assistant

A proprietary graphical program used to configure and update the firmware of the S1100 edge devices.

Decoder

See *Receiver*.

DHCP

(Dynamic Host Configuration Protocol) A communication protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in a network.

DVR

(Digital Video Recorder) A device (usually a computer) that acts like a VCR in that it has the ability to record and play back video images. The DVR takes the feed from a camera and records it into a digital format on a storage device which is most commonly the hard drive.

Edge Device

A Verint device transmitting or receiving video signals through an IP network. The devices can be wireless or wired; some transmitters are IP cameras.

Encoder

See *Transmitter*.

Ethernet

A local area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10, 100, and 1000 Mbps. It is one of the most widely implemented LAN standards. The 802.11 protocols are often referred to as “wireless Ethernet.”

Firmware

Software stored in read-only memory (ROM) or programmable ROM (PROM), therefore becoming a permanent part of a computing device.

H.264

Also known as MPEG-4 AVC (Advanced Video Coding), is a video compression standard that

offers significantly greater compression than its predecessors.

IP

(Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

LAN

(Local Area Network) A computer network that spans a relatively small area. A LAN can connect workstations, personal computers, and surveillance equipment (like edge devices). See also *WAN*.

MPEG-4

A graphics and video lossy compression algorithm standard that is derived from MPEG-1, MPEG-2, and H.263. MPEG-4 extends these earlier algorithms with synthesis of speech and video, fractal compression, computer visualization, and artificial intelligence-based image processing techniques.

Multicast

Communication between a sender and multiple receivers on a network; the devices can be located across multiple subnets, but not through the Internet. Multicast is a set of protocols using UDP/IP for transport.

NTSC

(National Television Standards Committee) The North American standard (525-line interlaced raster-scanned video) for the generation, transmission, and reception of television signals. In addition to North America, the NTSC standard is used in Central America, a number of South American countries, and some Asian countries, including Japan. Compare with *PAL*.

NTP

(Network Time Protocol) A protocol designed to synchronize the clocks of devices over a network.

OSD

(On-screen Display) Status information displayed on the video monitor connected to a receiver edge device.

PAL

(Phase Alternation by Line) A television signal standard (625 lines) used in the United Kingdom, much of western Europe, several South American countries, some Middle East and Asian countries, several African countries, Australia, New Zealand, and other Pacific island countries. Compare with *NTSC*.

PEAP

(Protected Extensible Authentication Protocol) A method to securely transmit authentication information, including passwords, over a wireless network.

Point-to-Point Connection

The association of a transmitter and a receiver to view video coming from an analog camera on an analog monitor.

PSK

(Pre-Shared Key) A mode of the WPA and WPA2 security protocols, designed for home and small office networks that cannot afford the cost and complexity of an authentication server. It is also known as *personal mode*.

PTL

(Push-To-Listen) In a two-way system, the communication mode in which the listener must push a button while listening.

PTT

(push-To-Talk) In a two-way system, the communication mode in which the talker must push a button while talking.

PTZ Camera

(Pan-Tilt-Zoom) An electronic camera that can be rotated left, right, up, or down as well as zoomed in to get a magnified view of an object or area. A PTZ camera monitors a larger area than a fixed camera.

QoS

(Quality of Service) A set of low-level networking protocols giving higher priority to more important data flows while ensuring that the less important ones do not fail.

Receiver

A device converting a digital video signal into an analog form. Also called *decoder*.

Repeater

A range extender for wireless links.

RF

(Radio Frequency) Any frequency within the electromagnetic spectrum associated with radio wave propagation. When a modulated signal is supplied to an antenna, an electromagnetic field is created that is able to propagate through space. Many wireless technologies are based on RF field propagation.

RS-232

A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices.

RS-422

A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices, designed to replace the older RS-232 standard because it supports higher data rates and greater immunity to electrical interference.

RS-485

An Electronics Industry Alliance (EIA) standard for multipoint communications.

SConfigurator

A proprietary graphical program used to configure and update the firmware of edge devices.

Serial Port

An interface that can be used for serial communication, in which only one bit is transmitted at a time. A serial port is a general-purpose interface that can be used for almost any type of device.

SSL

(Secure Sockets Layer) A commonly used protocol for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. The SSL protocol secures the following data: I/O, serial port, and VSIP communication; it does not apply to audio and video transmission.

TKIP

(Temporal Key Integrity Protocol) A security protocol used in the WPA authentication method.

TLS

(Transport Layer Security) A cryptographic protocol that provide secure communications on a wireless network.

Transceiver

(Transmitter/Receiver) A device that both transmits and receives analog or digital signals.

Transmitter

A device sending video signals captured with a connected camera to a receiver. The transmitter converts the analog signal into a digital form before transmitting it. Also called *encoder*.

TTLS

(Tunneled Transport Layer Security) A cryptographic protocol that creates a secure TLS tunnel.

VSIP

(Video Services over IP) A proprietary communication protocol for sending messages between a computer and a Verint edge device, or between two devices.

WAN

(Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

WEP

(Wired Equivalent Privacy) A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. It is designed to afford wireless networks the same level of protection as a comparable wired network.

Wireless Bridge

A link between two networks, wired or wireless.

Wireless Cell

A group of wireless devices that communicate together on the same radio frequency channel and share the same wireless passkey.

Wireless Transmission

A technology in which electronic devices send information to receivers using radio waves rather than wiring.

WPA

(Wi-Fi Protected Access version 1) An authentication method to secure wireless systems. It is the successor of WEP. WPA implements the majority of the IEEE 802.11i standard.

WPA2

(Wi-Fi Protected Access version 2) An authentication method that implements the full 802.11i standard, but will not work with some older network cards. It is also known as *802.11i*.

Index

Numerics

802.11 25, 29–32
802.11i 30

A

address, IP. *See* IP address.
AES Encryption
    SNMP Setting 23, 61
AES-CCMP 30
AES-OCB 29
alarm configuration 55, 63
aligning an antenna 73
antenna alignment 73
antenna gain 27
APIPA
    addressing 17
APIPA addressing scheme 8, 17, 86
APIPA device 8
audio mode in a connection 64
audio parameters 44
authentication 30
Authentication Type
    MD5 Authentication
        SNMP Setting 23, 61
    No Authentication
        SNMP Setting 23, 61
    Password
        SNMP Setting 23, 61
    SHA Authentication
        SNMP Setting 23, 61
    SNMP Setting 23, 61

B

Backup Trap Destination Address
    SNMP Setting 22, 60
band, frequency 26
bandwidth, channel 26, 52
batch network configuration 59
baud rate, serial port 42
bias 45
bit rate
    RF. *See* wireless bit rate.
    video 37
    wireless. *See* wireless bit rate.
bridge. *See* S3100 series.
brightness 36
broadcast detection method
    in a device 19
    in SConfigurator 4, 9

C

camera, IP. *See* edge device.
certificate
    802.11 32
    SSL 67
channel bandwidth 26, 52
channel, RF 26
CIF resolution 38
CLI (command line interface) 87, 88
client
    changing the wireless bit rate 33
    list of 33
columns in the Units box 11
COM port 88
command line interface (CLI) 87
common VSIP port 4, 9
Community Name
    SNMP Setting 22, 60
compression
    audio input 45
    video, mode 39
computer requirements 2
configuration
    alarm 55, 63
    batch network 59
    default 15, 56
    edge device 14–46
    point-to-point repeater 50
    point-to-point system 49
Configuring S1816e-SP Encoder 57
connection
    point-to-point 63–65
    secure. *See* SSL connection.

serial port, for the CLI 88
SSL. *See* SSL connection.
transmitter and receiver 63–65
VSIP. *See* VSIP connection.
console, Verint 88
contrast 36
country of operation 15

D

data bit 42
default value
resetting to 15, 56
SSL passkey 67
VSIP port 4
DES Encryption
SNMP Setting 23, 61
detecting edge devices. *See* discovery process *or* discovery IP address.
device. *See* edge device.
DFS (Dynamic Frequency Selection) 15
DHCP (Dynamic Host Configuration Protocol) 17, 59
digital SSL certificate 67
discovery IP address
in a device 19
in SConfigurator 4, 9
discovery process
all devices on LAN 4, 7–9, 83
many devices 7–10
new devices 4, 7–9, 83
one device 9, 10
distance, maximum link 27
downgrade of firmware 70
duplex audio mode 64

E

EAP (Extensible Authentication Protocol) 30
edge device
accessible to SConfigurator iii
APIPA 8
available parameters 14
changing the name 15
configuring 14–46
configuring many at the same time 59
discovering 4, 7–10, 83
identifying 15
information to display 11
list of iii
rebooting 15
troubleshooting 82–84
emitting power 27
encoder parameters 37–40
encryption 30
Enterprise mode, WPA or WPA2 30
error messages during firmware update 71–72
Ethernet parameters
in a device 17
in SConfigurator 4

F

factory default configuration 15, 56
filter
IP 34
noise reduction 39
video 39
firmware
downgrading 70
version, displayed 15
firmware update
messages 71–72
performing 69–71
preventing 21
with serial port 71
forced bit rate 33
frame rate 37, 50
frequency band 26
frequency channel 26
full duplex audio mode 64

G

gain
antenna 27
audio 45
gateway, IP address 17
general parameters 15

H

hue 36

I

I/O data 63

identifying a device 15
I-frame 38
information on edge devices 11
input compression 45
input filter mode 39
input type, audio 45
input, video 36
installation 2
intra interval 38
IP Address
    APIPA 17
    Backup Trap Destination
        SNMP Setting 22, 60
    Primary Trap Destination
        SNMP Setting 22, 60
IP address
    APIPA 17, 86
    computer 4
    discovery 4
    edge device 17
    gateway 17
    SConfigurator 4
    subnet mask 17
    temporary 17, 86
IP camera. *See* edge devide.
IP filtering parameters 34
IP link
    securing 67–68
IP parameters
    in a device 17
    in SConfigurator 4

K

key
    encryption 31
    SSL. *See* SSL passkey.
    WEP 31
    wireless 29
    WPA 31

L

license 11, 76–81
link distance, maximum 27
link speed. *See* wireless bit rate.
link status 33
list of trusted devices
    adding a device 68
    creating 6
    indicator in the Units box 11
    troubleshooting 83
loading default configuration 15, 56
lost device 8

M

MAC mode 25, 29–32
margin, minimum RF 27
mask, subnet 17
master, list of connected clients and slaves 33
maximum link distance 27
messages, during firmware update 71–72
minimum RF margin 27
mode
    MAC 25, 29–32
    RS-422/485 42
multicast detection method
    in a device 19
    in SConfigurator 4, 9
multiport S17XXe series. *See* edge device.

N

name of device 15, 51
network configuration, batch 59
network parameters
    for a batch of devices 59
    in a device 17–34
    in SConfigurator 4
noise reduction filter 39
NTSC 35

O

operating mode, serial port 42
order, starting 27, 52

P

packages for licensing 76, 79
PAL 35
parameters
    audio 44
    filtering 34
    IP filtering 34

network 17–34
RF (radio frequency) 25–34
SConfigurator 4–7
serial port 42
SSL. *See* SSL parameters.
system status 15
video 35–41
VSIP. *See* VSIP parameters.
wireless 25–34
parity 42
passkey
encryption 31
SSL. *See* SSL passkey.
WEP 31
wireless 29
WPA 31
PEAP (Protected Extensible Authentication Protocol) 30
personal mode, WPA or WPA2 30
point-to-point connection 63–65
point-to-point repeater 50, 51
port
COM. *See* COM port.
serial. *See* serial port.
VSIP. *See* VSIP port.
power, transmission 27
preventing firmware update 21
Primary Trap Destination Address
SNMP Setting 22, 60
Privacy Password
SNMP Setting 23, 61
Privacy Protocol
AES Encryption
SNMP Setting 23, 61
DES Encryption
SNMP Setting 23, 61
No Encryption
SNMP Setting 23, 61
SNMP Setting 23, 61
product type 11
program options 4–7
PSK (Pre-Shared Key) 30
PTT/PTL mode 64
push-to-listen mode 64
push-to-talk mode 64

Q

quality, video 50, 54
quantizer 37

R

radio frequency. *See* wireless parameters.
radio transmission power 27
rate control, video 38
rebooting the device 15
removal code for a license 81
repeater, point-to-point 50, 51
requirements, computer 2
reserved VSIP ports 4
reset to factory default 15, 56
resolution, video 38, 50
RF (radio frequency). *See* wireless parameters.
role of the wireless device 25
RS-232 parameters 42
RS-422/485 parameters 42

S

S1100, configuration context 14
S1100w. *See* edge device.
S1504e-R. See edge device.
S1708e series. *See* edge device.
S17XXe series. *See* edge device.
S1816e-SP Encoder
Configuring 57
S1900e series. *See* edge device.
S1900e-Vicon. *See* edge device.
S2500e. *See* edge device.
S2600e series. *See* edge device.
S2700e series. *See* edge device.
S2750e series. *See* edge device.
S3100 series. *See* edge device.
S4100 series
configuring 47
resetting the configuration 56
S4200 series. *See edge device.*
S4300 series. *See edge device.*
saturation, video 36
scenarios for device discovery 8–9
SDCF 25
Secure Sockets Layer. *See the SSL entries.*
secure VSIP connection. *See* SSL connection.
security
defined 66–68
indicator in the Units box 11
parameters for the wireless devices 29–32
in SConfigurator 6
sensitivity threshold 27, 53
serial port
data in a connection 63

for firmware update 71
method to access the CLI 88
parameters 42
Setting
SNMP 22
Authentication Type 23, 61
MD5 Authentication 23, 61
No Authentication 23, 61
Password 23, 61
SHA Authentication 23, 61
Backup Trap Destination Address 22, 60
Community Name 22, 60
Primary Trap Destination Address 22, 60
Privacy Password 23, 61
Privacy Protocol 23, 61
AES Encryption 23, 61
DES Encryption 23, 61
No Encryption 23, 61
System Contact 22, 60
System Location 22, 60
User Name 22, 61
Setting The Vsip 22
single device, discovering 9, 10
slave
aligning the antenna 73
changing the wireless bit rate 33
list of 33
SNMP
Setting 22
Authentication Type 23, 61
MD5 Authentication 23, 61
No Authentication 23, 61
Password 23, 61
SHA Authentication 23, 61
Backup Trap Destination Address 22, 60
Community Name 22, 60
Primary Trap Destination Address 22, 60
Privacy Password 23, 61
Privacy Protocol 23, 61
AES Encryption 23, 61
DES Encryption 23, 61
No Encryption 23, 61
System Contact 22, 60
System Location 22, 60
User Name 22, 61
SPCF 25
speed of the wireless link. *See* wireless bit rate.
SSID (service set ID) 26
SSL certificate 67
SSL connection
defined 67
indicator in the Units box 11
troubleshooting 83–84
SSL parameters
in a device 21
in SConfigurator 6
SSL passkey
defined 67
in a device 21
in SConfigurator 6
troubleshooting 83–84
SSL security. *See* security.
standard, television display 35
starting order 27, 52
starting SConfigurator 2
status messages during firmware update 71–72
status, system 15
stop bit 42
subnet mask 17
System Contact
SNMP Setting 22, 60
System Location
SNMP Setting 22, 60
system status parameters 15

T

target frame rate 37
target video bit rate 37
TCP connection 83
television display standard 35
Telnet 21, 88
temperature, board 11
temporary IP address 17, 86
threshold, sensitivity 27, 53
timeout, CLI 89
TKIP (Temporal Key Integrity Protocol) 30
TLS (Transport Layer Security) 30
TPC (Transmit Power Control) 15
transmission distance, maximum 27
transmission power 27
troubleshooting a device 82–84
trusted device list
adding a device 68
creating 6
indicator in the Units box 11
troubleshooting 83
TTLS (Tunneled Transport Layer Security) 30
type, device 11

U

UDP connection 83
unicast detection method 9

up time 11
updating firmware
    messages 71–72
    performing 69–71
    preventing 21
    with serial port 71
User Name
    SNMP Setting 22, 61

V

Verint console 88
version of firmware 15
video bit rate 37
video encoder parameters 37–40
video feed filtering 39
video input 36
video mode in a connection 64
video parameters 35–41
video quality 54
VSIP connection
    defined 11
    secure 67
    troubleshooting 83–84
VSIP parameters
    in a device 19
    in SConfigurator 4
VSIP port
    common 4, 9
    default 4
    in the discovery process 7–9
    reserved 4
    troubleshooting 83
    See also VSIP parameters.

W

WEP (Wired Equivalent Privacy) 30
wired edge device, list of iii
wireless bit rate
    changing, for a client or slave 33
    S1100w 26
    slave 26
wireless edge device, list of iii
wireless link status 33
wireless parameters 25–34
WPA (Wi-Fi Protected Access) 30
WPA2 (Wi-Fi Protected Access version 2) 30

VERINT

POWERING ACTIONABLE INTELLIGENCE®

For more information, please visit us at www.verint.com/video_solutions

Americas: info@verint.com
EMEA: marketing.emea@verint.com
APAC: marketing.apac@verint.com

All other trademarks and product names are the property of their respective owners.
The information in this document may be superseded by subsequent documents.

Revision 2